(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年6 月23 日 (23.06.2005)

PCT

(10) 国際公開番号
WO 2005/057865 A1

(51) 国際特許分類[7]: H04L 12/56

(21) 国際出願番号: PCT/JP2004/018491

(22) 国際出願日: 2004 年12 月10 日 (10.12.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2003-412979 2003 年12 月11 日 (11.12.2003) JP
特願2004-261033 2004 年9 月8 日 (08.09.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

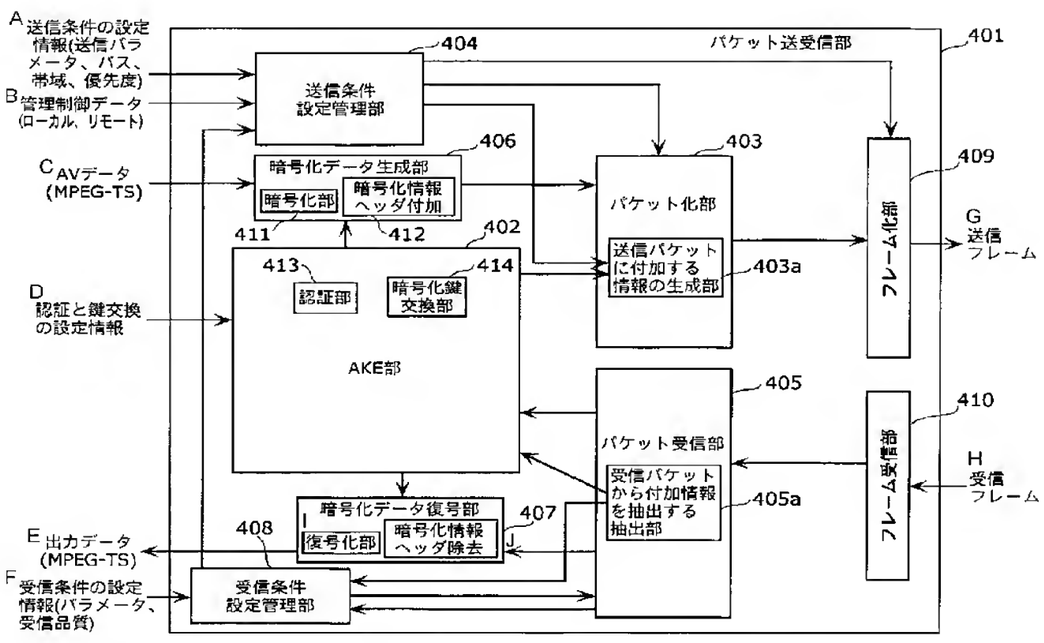
(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 森岡 芳宏 (MORIOKA, Yoshihiro). 綾木 靖 (AYAKI, Yasushi). 臼木 直司 (USUKI, Naoshi).

(74) 代理人: 新居 広守 (NII, Hiromori); 〒5320011 大阪府大阪市淀川区西中島３丁目１１番２６号 新大阪末広センタービル３Ｆ 新居国際特許事務所内 Osaka (JP).

[続葉有]

(54) Title: PACKET TRANSMITTER APPARATUS

(54) 発明の名称: パケット送信装置



A... TRANSMISSION CONDITION SETTING INFORMATION (TRANSMISSION PARAMETERS, BUS, BAND AND PRIORITY)
B... MANAGEMENT CONTROL DATA (LOCAL AND REMOTE)
C... A/V DATA (MPEG-TS)
D... AUTHENTICATION AND KEY EXCHANGE SETTING INFORMATION
E... OUTPUT DATA (MPEG-TS)
F... RECEPTION CONDITION SETTING INFORMATION (PARAMETERS AND RECEPTION QUALITY)
404... TRANSMISSION CONDITION SETTING/MANAGING PART
406... ENCRYPTED DATA PRODUCING PART
411... ENCRYPTING PART
412... ENCRYPTED INFORMATION HEADER ADDITION
402... AKE PART
413... AUTHENTICATING PART
414... ENCRYPTION KEY EXCHANGING PART
407... ENCRYPTED DATA DECRYPTING PART
I... DECRYPTING PART
J... ENCRYPTED INFORMATION HEADER REMOVAL
408... RECEPTION CONDITION SETTING/MANAGING PART
403... PACKETIZING PART
403a... PART FOR PRODUCING INFORMATION TO BE ADDED TO TRANSMITTED PACKET
405... PACKET RECEIVING PART
405a... EXTRACTING PART FOR EXTRACTING ADDED INFORMATION FROM RECEIVED PACKET
401... PACKET TRANSMITTING/RECEIVING PART
409... FRAMING PART
410... FRAME RECEIVING PART
G... TRANSMITTED FRAME
H... RECEIVED FRAME

(57) Abstract: A packet transmitter apparatus capable of transmitting, by use of widely utilized packets such as IP packets and the like, contents protected by content protection technologies such as DTCP and the like. There are included a transmission condition setting/managing part (404) for extracting, from received non-A/V data or A/V data, at least one of A/V data billing information, reproduction control information and copy control information and for producing, from the extracted information, encryption mode information indicative of an encryption mode that is a condition when A/V data are transmitted; an encrypted data producing part (406) for producing encrypted data by encrypting, based on a transmission condition as decided by a combination of input terminal information, data format information and attribute information, the received A/V data and further by adding, to the encrypted A/V data, an encryption information header based on the encryption mode information; and a packetizing part (403) for producing a packet by adding a packet header to the produced encrypted data.

(57) 要約: ＤＴＣＰ等のコンテンツ保護技術で保護されたコンテンツをＩＰパケット等の広く普及したパケットで送信することが可能なパケット送信装置を提供する。 入力された非ＡＶデータまたはＡＶデータより、ＡＶデータの課金情報、再生制御情報およびコピー制御情報の少なくとも１つの情報を抽出し、抽出した情報から、ＡＶデータを送信する際の条件となる暗号化モードを示す暗号化モード情報を生成する送信条件設定管理部４０４と、入力端子情報、データフォーマット情報および属性情報を組み合わせて決定される送信条件に基づいて、入力されたＡＶデータを暗号化し、暗号化されたＡＶデータに対して暗号化モード情報に基づく暗号化情報ヘッダを付加することによって暗号化データを生成する暗号化データ生成部４０６と、生成された暗号化データに対して、パケットヘッダを付加することによってパケットを生成するパケット化部４０３とを備える。

[続葉有]

WO 2005/057865 A1

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

パケット送信装置

技術分野

[0001] 本発明は、IEEE802．3などのイーサネット(登録商標)(有線LAN)やIEEE802．11などの無線LANなどを用いて、暗号化されたAVストリームをIPパケット化して高品質に送信するパケット送信装置に関する。

背景技術

[0002] 近年の通信技術の発展に伴い、効率よくパケットを伝送する様々な技術が提案されている(例えば、特許文献1参照)。その一つとして、従来、一般家庭において、部屋内でデジタル放送チューナやDVHS方式ビデオレコーダー間をIEEE 1394方式デジタルインターフェースで接続し、IEC 61883−4で規定されたMPEG−TS(Moving Picture Experts Group／Transport Stream)信号の伝送が行われている。ここで、放送コンテンツにコピーワンジェネレーション(Copy One Generation)などコンテンツ保護がかかっている場合、コンテンツを不正コピーから保護するため、コンテンツを暗号化して伝送している。この様にデジタル放送を受信・選局して得られたMPEG−TSなどのAVデータを暗号化して伝送する方式の一例として、DTCP(Digital Transmission Content Protection)方式が規定されている。DTCPは、IEEE1394やUSBなどの伝送メディア上のコンテンツ保護技術である。DTCP方式は、DTLA(Digital Transmission Licencing Administrator)で規格化された方式であり、 HYPERLINK"http:／／www. dtcp. com" http:／／www. dtcp. com、 HYPERLINK "http:／／www. dtcp. com／data／dtcp#tut. pdf" http:／／www. dtcp. com／data／dtcp#tut. pdf、HYPERLINK "http:／／www. dtcp. com／data／wp#spec. pdf" http:／／www. dtcp. com／data／wp#spec. pdfや、書籍「IEEE1394、AV機器への応用」、高田信司監修、日刊工業新聞社、「第8章、コピープロテクション」、133ー149ページで説明されている。

[0003] MPEG−TSについて説明する。トランスポートストリームはトランスポートパケット(T

S packet)が複数個集まったものである。TS packetは188byteの固定長パケットで、その長さはATMのセル長との整合性およびリードソロモン符号などの誤り訂正符号化を行なう場合の適用性を考慮して決定されている。TS packetは4byte固定長のパケットヘッダと可変長のアダプテーションフィールド(adaptation field)およびペイロード(payload)で構成される。パケットヘッダにはPID(パケット識別子)や各種のフラグが定義されている。このPIDによりTS packetの種類を識別する。adaptation_fieldとpayloadは、片方のみが存在する場合と両方が存在する場合があり、その有無はパケットヘッダ内のフラグ(adaptation_field_control)により識別できる。adaptation_fieldは、PCR(Program_Clock_Reference)等の情報伝送およびTS packetを188byte固定長にするためのTS packet内でのスタッフィング機能を持つ。また、PCRは27MHzのタイムスタンプで、符号化した時の基準時間を復号器のSTCで再現するためにPCRの値が参照される。MPEG−2のTSでは復号器のSTC(System Time Clock)はPCRによるPLL動機機能を持つ。このPLL同期の動作を安定させるためにPCRの送信間隔は最大0．1msである。映像や音声などの個別ストリームが収められたMPEGのPESパケットは同じPID番号を持つ複数のTS packetのpayloadに分割して伝送する。また、PESパケットの先頭は、TS packetの先頭から開始するように構成される。トランスポートストリームは複数のプログラムを伝送することができるため、ストリームに含まれているプログラムとそのプログラムを構成している映像や音声ストリームなどのプログラムの要素との関係を表すテーブル情報が用いられる。このテーブル情報はPSI(Program Specific Information)と呼ばれ、PAT (Program Association Table)、PMT(Program Map Table)などのテーブルを用いる。PAT、PMTなどのPSIはセクションと呼ばれる単位でTS packetの中のpayloadに配置されて伝送される。PATにはプログラム番号に対応したPMTのPIDなどが指定されており、PMTには対応するプログラムに含まれる映像、音声、付加データおよびPCRのPIDが記述されるため、PATとPMTを参照することにより、ストリームの中から目的のプログラムを構成するTS packetだけを取り出すことができる。TSに関する参考文献としては、例えば、CQ出版社、TECHＩ Vo．4、「画像＆音声圧縮技術のすべて(インターネット／ディジタルテレビ、モ

バイル通信時代の必須技術)」、監修、藤原洋、第6章、「画像や音声を多重化するMPEGシステム」があり、同書にて解説されている。

[0004] PSIやSIに関する論理的な階層構造、処理手順の例、選局処理の例に関して、「ディジタル放送受信機における選局技術」、三宅他、三洋電機技報、VOL. 36、JUNE 2004、第74号、31ページから44ページにて解説されている。

[0005] また、デジタル放送で使用されるアクセス制御方式に関し、スクランブル、関連情報の仕様及びそれに関わる受信機仕様については、ARIB規格、ARIB STD−B25において規定されており、その運用については、ARIB技術資料、ARIB TR−B14およびARIB TR−B15において規定されている。

[0006] 図1(a)は、DTCP方式を用いたMPEG−TSのIEEE1394での伝送の一例である。DTCP方式では、送信側(パケット送信機器)をソース1801、受信側(パケット受信機器)をシンク1802と呼び、暗号化したMPEG−TSなどのコンテンツをソース1801からネットワーク1803を介して、シンク1802へ伝送している。図1(b)に、補足情報として、ソース機器およびシンク機器の例を併記する。

[0007] 図2は、DTCP方式における従来のパケット通信部の概略を説明する図であり、ここでは、図1のソース1801が備えるパケット送信部およびシンク1802が備えるパケット受信部の両方がパケット送受信部として示されている。まず、DTCP方式に準拠した認証と鍵交換(Authentification and Key Exchange、AKEと略する)が行なわれる。AKE部1901に対して、その認証と鍵交換の設定情報が入力され、この情報がパケット化部1902に伝達され、パケット化部1902において規定のヘッダが付加されたパケット化が行われ、ネットワーク1907に出力される。ここで、パケット化部1902は、送信条件設定部1903により決定された送信パラメータにより、入力データのパケット化および送信を行なう。受信側では、ネットワーク1907より入力する信号がパケット受信部1904でパケットヘッダなどの識別によりフィルタリングされ、AKE部1901に入力される。これにより送信側(ソース)のAKE部と、受信側(シンク)のAKE部がネットワーク1803および1907を介してお互いにメッセージの通信ができる。すなわち、DTCP方式の手順に従い、認証と鍵交換を実行する。

[0008] 送信側(ソース)と、受信側(シンク)で認証と鍵交換が成立すれば、次に、AVデー

タの伝送を行なう。ソースでは、MPEG—TS信号を暗号化部1905に入力して、MPEG—TS信号を暗号化した後、この暗号化されたMPEG—TS信号をパケット化部1902に入力し、ネットワーク1907に出力する。シンクでは、ネットワーク1907より入力する信号がパケット受信部1904でパケットヘッダなどの識別によりフィルタリングされ、復号部1906に入力され、復号されMPEG—TS信号が出力される。

[0009] 次に、図3を用いて上記手順を補足説明する。図3において、ソースとシンク間はIEEE1394で接続されている。まず、ソース側でコンテンツの送信要求が発生する。そして、ソースからシンクへ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。シンクは、コンテンツのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、認証要求をソースに送る。ソースとシンクはDTCP所定の処理により認証鍵の共有を図る。そして、ソースは認証鍵を用いて交換鍵を暗号化してシンクに送り、シンクで交換鍵が復号される。ソースでは暗号鍵を時間的に変化させるために、時間的に変化するシード情報を生成し、シンクに送信する。ソースでは、交換鍵とシード情報より暗号化鍵を生成して、MPEG—TSをこの暗号化鍵を用いて暗号化部で暗号化してシンクに送信する。シンクはシード情報を受信し交換鍵とシード情報より復号鍵を復元する。シンクではこの復号鍵を用いて暗号化されたMPEG—TS信号を復号する。

[0010] 図4は、図1においてMPEG—TS信号を伝送する場合のIEEE1394アイソクロナスパケットの一例である。このパケットは、4バイト(32ビット)のヘッダ、4バイト(32ビット)のヘッダCRC、224バイトのデータフィールド、4バイト(32ニット)のトレイラによって構成されている。暗号化されて伝送されるのは224バイトのデータフィールドを構成するCIPヘッダとTS信号のうち、TS信号のみで、他のデータは暗号化されない。ここで、DTCP方式固有の情報は、コピー保護情報である2ビットのEMI(Encription Mode Indicator)、およびシード情報のLSBビットであるO／E(Odd／Even)であり、これらは上記32ビットのヘッダ内に存在するため暗号化されずに伝送される。

[0011] しかしながら、上記従来の技術では、以下のような問題点を有している。従来のDTCP方式はIEEE1394において、アイソクロナスパケットを用いて伝送するためMPEG—TS信号のリアルタイム伝送ができるが、インターネットの標準プロトコルであるInt

ernet Protocol(IP)を用いて、イーサネット(登録商標)(IEEE802．3)、無線LAN(IEEE802．11)や、その他のIPパケットを伝送可能なネットワークで伝送ができないという大きな問題点がある。

[0012] すなわち、IPを介して論理的に接続されたパケット送信機器とパケット受信機器の間を、地上波／BSデジタル放送やサーバ型放送などデジタル著作権保護対応のコンテンツを著作権保護しつつ伝送できないという大きな問題点がある。

[0013] また、ライブ放送の伝送において、HTTP(HyperText Transfer Protocol)を用いる場合、HTTPリクエストの度に、前記暗号化に関して付加するヘッダ長や伝送コンテンツ長を受信側で計算する必要があり、受信側の処理が重いという課題がある。

[0014] さらに、ハードディスクなどに蓄積されたコンテンツを早送り、巻き戻し、スロー再生などの特殊再生を簡単に実現することが困難であるという問題点がある。

[0015] さらに、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツを共通の方法で簡単に、早送り、巻き戻し、スロー再生などの特殊再生することが困難であるという問題点がある。なお、ネットワーク経由ではなくローカル(機器本体)での操作に関しては、一例として、Blu—rayディスク方式の本体()での特殊再生などに関して、松下テクニカルジャーナル、2004年10月、34ページから38ページ、「Bru—ray Disk Rewritable Format(2) ー論理規格、著作権保護規格ー」において特殊再生のためのEP__mapデータ構造などが解説されている。

[0016] 特に、家庭内においては、放送等によって取得したデジタル著作権保護対応のコンテンツをデジタルTVやホームサーバ等が家庭内に設置された様々な機器に配信する必要がある。したがって、家庭内においては、コンテンツの著作権を保護しつつ、様々なメーカーの機器間でのコンテンツ転送を可能にするために、広く普及したIPパケットでDTCP方式に対応したコンテンツの配信、つまり、DTCP—IP(Digital Transmission Contents Protection over IP)を実現する必要がある。

特許文献1:特開2000—59463号公報

発明の開示

発明が解決しようとする課題

[0017] そこで、本発明は、DTCP等のコンテンツ保護技術で保護されたコンテンツをHTTPプロトコルやRTPプロトコルなどを利用してIPパケット等の広く普及したパケットで送信することが可能なパケット送信装置を提供することを目的とする。

課題を解決するための手段

[0018] 上記目的を達成するために、本発明に係るパケット送信装置は、パケット受信装置にパケットデータを送信するパケット送信装置であって、AVデータが入力される端子を示す入力端子情報、前記AVデータのデータフォーマットを示すデータフォーマット情報及び前記AVデータの属性を示す属性情報を含むAVデータ情報を取得するAVデータ情報取得手段と、前記AVデータ及び非AVデータの入力を受け付けるデータ入力手段と、前記非AVデータまたは前記AVデータより、前記AVデータの課金情報、再生制御情報及びコピー制御情報の少なくとも1つの情報を抽出し、抽出した情報から、前記AVデータを送信する際の条件となる暗号化モードを示す暗号化モード情報を生成する送信条件設定管理手段と、前記入力端子情報、前記データフォーマット情報及び前記属性情報を組み合わせて決定される送信条件に基づいて、前記データ入力手段より入力された前記AVデータを暗号化し、暗号化された前記AVデータに対して前記暗号化モード情報に基づく暗号化情報ヘッダを付加することによって暗号化データを生成する暗号化データ生成手段と、前記暗号化データ生成手段により生成された暗号化データに対して、パケットヘッダを付加することによってパケットを生成するパケット化手段と、前記パケット受信装置との間で認証処理を行う認証手段と、前記入力端子情報、前記属性情報及び前記パケット受信装置より指定される送信モードを示す情報の少なくとも1つを用いて、前記パケット送信装置と前記パケット受信装置の間での前記AVデータの伝送プロトコルを決定する伝送プロトコル決定手段と、前記認証処理によって前記パケット受信装置との認証処理が完了した後に、前記伝送プロトコル決定手段によって決定された伝送プロトコルに従って、前記パケット化手段によって生成された暗号化データを含むパケットを前記パケット受信装置に伝送する伝送手段とを備えることを特徴とする。

[0019] より具体的には、本願第1の発明は、AVデータと非AVデータとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、規定の送受信条件によ

り「暗号化または暗号化情報ヘッダ付加の実行を行う」暗号化データ生成手段と、パケットヘッダ付加手段とを具備するパケット送受信手段において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダ付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、および、前記暗号化情報ヘッダ付加手段において暗号化情報ヘッダ付加を行うか行わないかを制御する手段とを具備する。これにより、MPEG—TS信号などのAVストリームを外部から与えられる一定規則による送信条件に従い暗号化モードを決め、さらに暗号化情報ヘッダを付加することを決めることにより、パケット送受信機器間での信号の互換性を確保しながら、HTTPプロトコルやRTPプロトコルなどを利用しながらAVストリームの秘匿性を保つことが可能となる。

[0020] 本願第2の発明は、第1の発明における認証手段において、認証を実行するモードは、外部より入力される制御情報により決定する。たとえば、外部より入力される制御情報として、コンテンツ毎にアクセス位置を指定するURI(Uniform Resource Identifier)を与え、そのURIの形式により認証モードを決定する。たとえば、URIがQueryにより拡張されている場合は、認証が必要であり、そのQuery情報より認証用のTCP(Transmission Control Protocol)ポート番号を与えることが可能となる。これにより、認証実行モードを、外部より入力される制御情報により決定することが可能となる。

[0021] 本願第3の発明は、第1の発明における暗号化データ生成手段において、外部から与えられる規定の送信条件としてそのAVストリームのコピー制御情報(CCI;Copy Control Information)に従うことを特徴とし、暗号化モードと暗号化情報ヘッダ付加を決定する。これにより、MPEG—TS信号などのAVストリームをそのコピー制御情報に従い暗号化モードを決め、暗号化情報ヘッダを付加した後、パケット化して伝送するので、AVコンテンツの著作権者が設定したコピー制御モードを継承してパケットの伝送がなされる。すなわち、一定規則による処理を行うため、AVコンテンツの著作権保護を図りつつ、パケット送受信機器間での信号の互換性を確保することが可能となる。

[0022] 本願第4の発明は、第1の発明において、AVデータと非AVデータとをそれぞれの

データバッファに入力し、2つのバッファの出力は優先制御して前記パケットヘッダ付加手段に出力する。たとえば、非AVデータがそのデータバッファでオーバーフローしない様に制御しながら、AVデータをそのデータバッファから優先して出力する。これにより、AVデータと非AVデータの内、重要性の高いデータを優先して送信することが可能となる。

[0023] 本願第5の発明は、第1の発明において、AVデータを構成するデータブロックにタイムスタンプを付加し、1つ以上のタイムスタンプ付データブロックをまとめてRTP(Real—time Transport Protocol)パケットのペイロード部またはHTTPパケットのペイロード部にマッピングする。たとえば、AVデータがMPEG—TSの場合、各TSパケットにタイムスタンプを付加し、複数のタイムスタンプ付TSパケットをまとめてRTPまたはHTTP上にマッピングする。たとえば、各TSパケットに付加するタイムスタンプのクロックはMPEGのシステムクロック周波数を用いることができる。TSパケットに付加されたタイムスタンプより、MPEG—TSのネットワーク伝送によりPCR(Program Clock Reference)に付加した伝送ジッターを除去して、受信側でのMPEGシステムクロックの再生を行うことが可能となる。

[0024] 本願第6の発明は、第1の発明において、AVデータのパケット化は、受信側からの制御により、RTPまたはHTTPで行うことを切替え制御すること。たとえば、AVデータのパケット化は、受信側のAVデータ出力がディスプレイ充てに出力される場合は遅延の小さいRTPを用い、受信側のAVデータ出力が記録メディアに蓄積される場合は再送によりパケット落ちを低減するHTTPを用いる。このように、切替え制御することにより受信側でディスプレイに出力する場合は低遅延でのAVコンテンツの伝送が可能となり、また、受信側で蓄積する場合はパケットロスによる信号欠落が補償された高品質なAVコンテンツの伝送が可能となる。

[0025] また、本願第7の発明は、課金処理などを含むRMP(Rights Management & Protection)などのデジタル著作権対応のAVデータおよび非AVデータとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、入力されるデジタル著作権規定より暗号化伝送モードを選択できる手段を具備する。すなわち、「暗号化または暗号化情報ヘッダ付加の実行を行う」暗号化データ生成手段と、パケ

ットヘッダ付加手段とを具備するパケット送受信手段において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダ付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、および、前記暗号化情報ヘッダ付加手段において暗号化情報ヘッダ付加を行うか行わないかを制御する手段とを具備する。

[0026] これにより、課金処理などを含むRMP情報などデジタル著作権対応のMPEG—TS信号などのAVストリームを外部から与えられる一定規則による送信条件に従い暗号化モードを決め、さらに暗号化情報ヘッダを付加することを決めることにより、パケット送受信機器間での信号の互換性を確保しながら、AVストリームの秘匿性を保つことが可能となる。

[0027] 本願第8の発明は、第7の発明において、ライブで放送されているコンテンツをHTTPのチャンク伝送方式で伝送することにより、前記暗号化に関して付加するヘッダ長や伝送コンテンツ長HTTPリクエストの度に、受信側（クライアント）で計算する必要がなくなり、受信側の処理を軽くすることができる。

[0028] 本願第9の発明は、第7の発明において、ハードディスクなどに蓄積されたコンテンツをHTTPのレンジリクエストを用いて伝送することにより、早送り、巻き戻し、スロー再生などの特殊再生を簡単に実現することができる。

[0029] さらに、本願第10の発明は、第9の発明において、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツの異なるI、P、Bピクチャのバイト位置情報、時刻情報より、共通フォーマットとしてのI、P、Bピクチャフレーム位置情報を生成することにより、高品質なスロー再生、早送り、巻き戻しなどの特殊再生を容易に実現することが可能となる。

[0030] なお、本発明は、このようなパケット送信装置として実現できるだけでなく、パケット送信方法として実現したり、パケット送信装置のためのプログラムとして実現したり、そのプログラムを記録したコンピュータ読み取り可能なCD—ROMなどの記録媒体としても実現できる。

発明の効果

[0031] 本願第1の発明によれば、外部から与えられる一定規則によりAVコンテンツの送信

の暗号化モードを決めることができる。さらに、暗号化情報ヘッダを付加ルールを決めることができるため、パケット送受信機器間でのAVストリームの秘匿性を保ちながら信号の互換性を確保することが可能となる。

[0032] 本願第2の発明によれば、第1の発明における認証手段において、認証実行モードを外部入力の制御情報より決定する。たとえば、外部より入力される制御情報として、コンテンツ毎にアクセス位置を指定するURIを与え、そのURIの形式により認証モードを決定することができる。一例として、URIがQuery形式により拡張されている場合には認証が必要という情報と、同時に、そのQuery情報より認証用のTCPポート番号の情報を与えることが可能となる。これにより、認証実行モードを、外部より入力される制御情報により決定することが可能となる。

[0033] 本願第3の発明によれば、第1の発明における暗号化データ生成手段において、外部から与えられる規定の送信条件としてそのAVストリームのコピー制御情報に従うことを特徴とし、暗号化モードと暗号化情報ヘッダ付加を決定する。これにより、MPEG—TS信号などのAVストリームをそのコピー制御情報に従い暗号化モードを決め、暗号化情報ヘッダを付加した後、パケット化して伝送するので、AVコンテンツの著作権者が設定したコピー制御モードを継承してパケットの伝送がなされる。すなわち、一定規則による処理を行うため、AVコンテンツの著作権保護を図りつつ、パケット送受信機器間での信号の互換性を確保することが可能となる。

[0034] 本願第4の発明によれば、第1の発明において、AVデータと非AVデータとをそれぞれのデータバッファに入力し、2つのバッファの出力は優先制御して前記パケットヘッダ付加手段に出力する。たとえば、非AVデータがそのデータバッファでオーバーフローしない様に制御しながら、AVデータをそのデータバッファから優先して出力する。これにより、AVデータと非AVデータの内、重要性の高いデータを優先して送信することが可能となる。

[0035] 本願第5の発明によれば、第1の発明において、AVデータを構成するデータブロックにタイムスタンプを付加し、1つ以上のタイムスタンプ付データブロックをまとめてRTPパケットのペイロード部またはHTTPパケットのペイロード部にマッピングする。たとえば、AVデータがMPEG—TSの場合、各TSパケットにタイムスタンプを付加し、複

数のタイムスタンプ付TSパケットをまとめてRTPまたはHTTP上にマッピングする。たとえば、各TSパケットに付加するタイムスタンプのクロックはMPEGのシステムクロック周波数を用いることができる。TSパケットに付加されたタイムスタンプより、MPEG—TSのネットワーク伝送によりPCRに付加した伝送ジッターを除去して、受信側でのMPEGシステムクロックの再生を行うことが可能となる。

[0036] 本願第6の発明によれば、第1の発明において、AVデータのパケット化は、受信側からの制御により、RTPまたはHTTPで行うことを切替え制御すること。たとえば、AVデータのパケット化は、受信側のAVデータ出力がディスプレイ充てに出力される場合は遅延の小さいRTPを用い、受信側のAVデータ出力が記録メディアに蓄積される場合は再送によりパケット落ちを低減するHTTPを用いる。このように、切替え制御することにより受信側でディスプレイに出力する場合は低遅延でのAVコンテンツの伝送が可能となり、また、受信側で蓄積する場合はパケットロスによる信号欠落が補償された高品質なAVコンテンツの伝送が可能となる。

[0037] また、上記発明によれば、ネットワークを用いたAVコンテンツの伝送に関して、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ(AVデータコンテンツ)の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるAVデータの販売、課金が可能となり、安全性の高いB—B(Business to Business)、B—C(Business to Consumer)のコンテンツ販売流通が可能となる。

[0038] また、上記発明によれば、AVコンテンツをハードウェアで伝送処理する場合にも、一般のデータパケットは従来通りCPUを用いてソフトウェア処理を行える。よって、ソフトウェアの追加により管理情報や制御情報などデータを一般データとして伝送させることができる。これらのデータ量は優先データであるAVデータに比べて非常に少ないので、マイコンなど安価なマイクロプロセッサで実現可能となり低コストなシステムを実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価なCPUや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できる。

[0039] また、本願第7の発明によれば、地上波放送、衛星放送、CATVやインターネット経由で受信するデジタル放送信号より検出、抽出できるAVコンテンツの属性情報を送信端末と受信端末間でUPnP(Universal Plug and Play)—AVやHTTPなどのデータ交換プロトコルを用いて伝送することにより、送信端末と受信端末間でのAVコンテンツを送信する場合の暗号化モード、コンテンツ属性情報の伝送方法を決めることができる。さらに、暗号化情報ヘッダの付加ルールを決められるため、パケット送受信機器間でのAVストリームの秘匿性を保ちながら信号の互換性を確保することが可能となる。UPnPやUPnP—AVの標準仕様は、http://upnp.orgで公開されている。http://upnp.orgにおいて、例えば、「MediaServer V 1.0 and MediaRenderer V 1.0」に関して、「MediaServer V 1.0」、「MediaRenderer V 1.0」、「ConnectionManager V 1.0」、「ContentDirectory V 1.0」、「RenderingControl V 1.0」、「AVTransport V 1.0」、「UPnP(登録商標) AV Architecture V .83」などの仕様書が公開されている。

[0040] また、ネットワークを用いたAVコンテンツの伝送に関して、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ(AVデータコンテンツ)の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるAVデータの販売、課金が可能となり、安全性の高いB—B、B—Cのコンテンツ販売流通が可能となる。

[0041] また、AVコンテンツをハードウェアで伝送処理する場合にも、一般のデータパケットは従来通りCPUを用いてソフトウェア処理を行える。よって、ソフトウェアの追加により管理情報や制御情報などデータを一般データとして伝送させることができる。これらのデータ量は優先データであるAVデータに比べて非常に少ないので、マイコンなど安価なマイクロプロセッサで実現可能となり低コストなシステムを実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価なCPUや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できる。

[0042] また、サーバ型放送のRMPで用いる課金情報などを含むRMPI(Rights Manag

ement & Protection Information)で視聴あるいはコピー制限されたコンテンツをRMPに対応していないクライアントにCNM(Copy No More)やCN(Copy Never)で見せることができ、サーバ型放送の普及を加速することができる。

[0043] 本願第8の発明によれば、ライブで放送されているコンテンツをHTTPのチャンク伝送方式で伝送することにより、前記暗号化に関して付加するヘッダ長や伝送コンテンツ長HTTPリクエストの度に、受信側(クライアント)で計算する必要がなくなり、受信側の処理を軽くできる。

[0044] 本願第9の発明によれば、ハードディスクなどに蓄積されたコンテンツをHTTPのレンジリクエストを用いて伝送することにより、早送り、巻き戻し、スロー再生などの特殊再生を簡単に実現できる。

[0045] さらに、本願第10の発明は、第9の発明において、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツの異なるIフレーム位置情報より、共通のIフレーム位置情報を生成することにより、簡単に、早送り、巻き戻し、スロー再生などの特殊再生が実現される。

図面の簡単な説明

[0046] [図1]図1は、従来技術における送受信システムの説明図である。

[図2]図2は、従来技術におけるパケット送受信部のブロック図である。

[図3]図3は、従来技術における鍵交換にDTCP方式を適用する場合のコンテンツ伝送手順の説明図である。

[図4]図4は、従来技術における1395アイソクロナスパケットの構成例を示す図である。

[図5]図5は、本発明を適用するシステムの一例を示す図である。

[図6]図6は、本発明のシステムにおける通信手順を示すフローチャートである。

[図7]図7は、認証と鍵交換にDTCP方式を適用する場合のコンテンツ伝送手順の説明図である。

[図8]図8は、イーサネット(登録商標)を用いる一般家庭に本発明を適用した場合の一例の説明図である。

[図9]図9は、本発明の実施の形態1におけるパケット送受信部のブロック図である。

[図10]図10は、本発明の実施の形態1におけるプロトコルスタックの説明図である。

[図11]図11は、本発明の実施の形態2におけるパケット送受信部のブロック図である。

[図12]図12は、本発明の実施の形態3におけるパケット送受信部のブロック図である。

[図13]図13は、本発明の実施の形態4におけるパケット送受信部のブロック図である。

[図14]図14は、本発明の実施の形態5におけるパケット送受信部のブロック図である。

[図15]図15は、本発明の実施の形態5におけるプロトコルスタックの説明図である。

[図16]図16は、本発明の実施の形態5におけるMPEG—TSのイーサネット(登録商標)フレーム構成仕様の例を示す図である。

[図17]図17は、本発明の実施の形態5の第1および第2の変形例におけるパケット送受信部のブロック図である。

[図18]図18は、本発明の実施の形態5の第1の変形例におけるパケット化部およびパケット受信部の説明図である。

[図19]図19は、本発明の実施の形態5の第1の変形例におけるDTCP方式による暗号化コンテンツの伝送手順を示すフローチャートである。

[図20]図20は、本発明の実施の形態5の第2の変形例におけるパケット化部およびパケット受信部の説明図である。

[図21]図21は、本発明の実施の形態5の第2の変形例におけるプロトコルスタックの説明図である。

[図22]図22は、エラー訂正方式がリードソロモン方式である場合の説明図である。

[図23]図23は、エラー訂正方式がパリティ方式である場合の説明図である。

[図24]図24は、本発明の実施の形態6におけるパケット送受信部のブロック図である。

[図25]図25は、本発明の実施の形態6におけるプロトコルスタックの説明図である。

[図26]図26は、本発明の実施の形態6の第1の変形例におけるパケット送受信部の

ブロック図である。

[図27]図27は、本発明の実施の形態6の第2の変形例におけるパケット送受信部のブロック図である。

[図28]図28は、本発明の実施の形態7および8におけるパケット送受信部のブロック図である。

[図29]図29は、本発明の実施の形態7におけるDTCP方式による暗号化コンテンツの伝送手順を示すフローチャートである。

[図30]図30は、本発明の実施の形態7におけるプロトコルスタックの説明図である。

[図31]図31は、本発明の実施の形態9におけるパケット送受信部の構成を示すブロック図である。

[図32]図32は、本発明の実施の形態10におけるパケット送受信部の構成を示すブロック図である。

[図33]図33は、ピクチャ情報ファイルの構成を示す図である。

符号の説明

[0047] 101 パケット送信機器

102 ルータ

103 パケット受信機器

401、401a－401h パケット送受信部

402 AKE部

403 パケット化部

404 送信条件設定管理部

405 パケット受信部

406 暗号化データ生成部

407 暗号化データ復号部

408 受信条件設定管理部

409 送信パケットのフレーム化部

410 フレーム受信部

2401、2401a－2401b パケット送受信部

2402 TSストリーム識別部

2403 送信条件設定管理部

2404 DRM設定管理部

2405 AKE部

2406 パケット化部

2407 暗号化データ復号部

2408 フレーム化部

2409 フレーム受信部

2410 パケット受信部

2411 DRMコンテンツ購入決済部

2412 コンテンツメタ情報

2413 コンテンツバッファ

2414 暗号化部

2415 暗号化情報ヘッダ付加部

2416 HTTP／RTPヘッダ付加部

2417 条件設定部

2418 復号化部

2701 蓄積部

発明を実施するための最良の形態

[0048] 以下、本発明の実施の形態について、図面を用いて詳細に説明する。

最初に本発明の位置付けを明確にするために適用される通信システム例の概略について説明する。

[0049] 図5は本発明を適用する通信システムの一例である。この通信システムは、パケットを送信するパケット送信機器101と、パケットのルーティングを行うルータ102と、パケットを受信するパケット受信機器103とから構成される。パケット送信機器101およびパケット受信機器103は、本発明に係る装置である。パケット送信機器101には、送受信条件の設定情報、認証と鍵交換の設定情報、入力ストリーム（MPEG—TSなどコンテンツ）が入力され、図6に示されるように、以下の手順1から3に基づき、ルータ1

02との間で通信を行う。

[0050] ＜手順1＞送受信パラメータの設定を行なう。

（手順1−1）パケット送受信機器のMAC（Media Access Control）アドレス、IPアドレス、TCP／UDP（User Datagram Protocol）ポート番号等を設定。

（手順1−2）送信信号の種別、帯域を設定。QoS（Quality of Service）エージェントとして動作するパケット送信機器101とパケット受信機器103、QoSマネージャとして動作するルータ102との間でIEEE802．1Q（VLAN；Virtual LAN）規格を用いたネットワークの運用に関する設定を実施。

（手順1−3）優先度の設定（IEEE802．1Q／pによる運用）

[0051] ＜手順2＞認証と鍵交換：

（手順2−1）認証と鍵交換を行なう。たとえば、DTCP方式を用いることもできる。

[0052] ＜手順3＞ストリーム伝送：

（手順3−1）パケット送信機器とパケット受信機器間での暗号化されたストリームコンテンツ（MPEG−TS）を伝送する。

[0053] なお、コンテンツの入力信号としてMPEG1／2／4などにおけるMPEG−TS，MPEG−PS（Program Stream）、MPEG−ES（Elementary Stream）、MPEG−PES（Packetized Elementarty Stream）などがある。

[0054] ここでは、例ではMPEG−TSを使用しているが、これに限らず本発明で用いる入力コンテンツの適用範囲としては、MPEG1／2／4などMPEG−TSストリーム（ISO／IEC13818）、DV（IEC61834、IEC61883）、SMPTE（Society of Motion Picture & Television Engineers） 314M（DV−based）、SMPTE259M（SDI）、SMPTE305M（SDTI）、SMPTE292M（HD−SDI）、ISO／IEC H．264等で規格化されているストリーム、さらには、一般的なAVコンテンツも適用可能である。

[0055] さらに、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、データ転送速度がコンテンツストリームの通常再生データレートよりも大きくなるなどの条件化において、リアルタイムより高速のコンテンツ伝送も可能である。

[0056] 次に、上記手順2の認証と鍵交換に関して補足説明する。図7において、パケット送信機器101とパケット受信機器103間はIPネットワークにより接続されている。まず、パケット送信機器101からパケット受信機器103へコンテンツのコピー保護情報を含んだコンテンツの保護モード情報が送信される。

[0057] パケット受信機器103は、コンテンツのコピー保護情報の解析を行い、使用する認証方式を決定して認証要求をパケット送信機器101に送る。

[0058] これらの処理を通してパケット送信機器101とパケット受信機器103は認証鍵を共有する。

[0059] 次に、パケット送信機器101は認証鍵を用いて交換鍵を暗号化してパケット受信機器103に送り、パケット受信機器103で交換鍵が復号される。

[0060] パケット送信機器101では暗号鍵を時間的に変化させるために、時間的に変化する鍵変更情報を生成し、パケット受信機器103に送信する。

[0061] パケット送信機器101では、交換鍵と鍵変更情報より暗号化鍵を生成して、MPEG—TSをこの暗号化鍵を用いて暗号化部で暗号化してパケット受信機器103に送信する。

[0062] パケット受信機器103は受信した鍵変更情報を交換鍵より復号鍵を復元する。パケット受信機器103ではこの復号鍵を用いて暗号化されたMPEG—TS信号を復号する。

[0063] 図8は、本方式をイーサネット(登録商標)によるLANを備える2階建ての家庭に適用した場合の一例である。この家庭は、1階に設置されたルータ303を含むネットワークシステム301と、2階に設置されたスイッチングハブ304を含むネットワークシステム302を備える。ネットワーク305は、ルータ303とスイッチングハブ304を接続するイーサネット(登録商標)ネットワークである。家庭内の全てのイーサネット(登録商標)ネットワークの帯域は100Mbpsである。

[0064] 1階の1階のネットワークシステム301の構成として、ルータ303には、テレビ(TV)、パソコン(PC)、DVDレコーダが100Mbpsのイーサネットで接続され、また、エアコン、冷蔵庫がECHONETで接続されている。

[0065] また、2階では、スイッチングハブ304にテレビ(TV)、パソコン(PC)、DVDレコー

ダが100Mbpsのイーサネットで接続され、また、エアコンがECHONETで接続されている。なお、ECHONETは「エコーネットコンソーシアム」(HYPERLINK ″http://www.echonet.gr.jp/″ http://www.echonet.gr.jp/)で開発されている伝送方式である。

[0066] なお、この家庭において、例えば、デジタル著作権保護の対象となるコンテンツを放送で受信し、家庭内の各機器(エアコン、DVD、PC、冷蔵庫)にIPパケットで配信するTVが本発明のパケット送信機器101に相当し、各機器がパケット受信機器103に相当する。

[0067] 図8において、パソコン(PC)、DVDレコーダ、ルータ303およびスイッチングハブ304は、IEEE802.1Q(VLAN)に対応している。すなわち、ルータ303およびスイッチングハブ304において、各ポートのデータレートが全て同じ(例えば100Mbps)場合、特定ポートへ出力されるデータ帯域の合計がそのポートの伝送レートの規格値または実力値を超えない限り、入力ポートへ入力されたデータはルータ(あるいは、スイッチングハブ)内部で失われず全て出力ポートに出力される。

[0068] スイッチングハブでは、たとえば8個の入力ポートにデータが同時に入力されても、それぞれのデータの出力ポートが異なっていれば、それぞれのデータはハブ内部のバッファで競合しないでスイッチングされて出力ポートより出力されるため、入力データはパケット落ちすることなく全て出力ポートに出力される。

[0069] 図8において、家庭内の全てのイーサネット(登録商標)の帯域が100Mbpsであるため、1階と2階間のネットワーク305の帯域も100Mbpsである。1階と2階の複数の機器間で複数のデータが流れる場合、各データに対する帯域制限がない場合、このネットワーク305上を流れるデータのデータレート合計が100Mbpsを超える可能性があり、MPEG—TSの映像アプリなどリアルタイム伝送が必要なストリームが途切れる可能性がある。この場合、リアルタイム伝送が必要なストリームが途切れない様にするには、伝送データに対して優先制御が必要である。

[0070] このような問題は、端末だけでなく、ルータやスイッチングハブにおいて、後述するストリーム伝送やファイル転送の速度制限機構などを導入することにより解決できる。

[0071] たとえば、MPEG—TSストリームの伝送優先度をファイル転送データの伝送優先度

よりも高くすると、1階と2階のPC間でのファイル転送をバックグラウンドで行いながら、同時に、1階および2階のDVDレコーダ、PC，TVの間でMPEG－TSを暗号化して、HTTPプロトコルやRTPプロトコルなどを利用してリアルタイムで伝送することが可能となる。

[0072] なお、HTTPプロトコル（IETF規格、RFC2616、RFC1945）の概要、構成、動作に関しては、たとえば、「連載：インターネット・プロトコル詳説（1）、HTTP（Hyper Text Transfer Protocol）ー前編」、WEB資料、http：／／www. atmarkit. co. jp／fnetwork／rensai／netpro01／netpro01. htmlで解説されている。

[0073] 前述したルータ303、またはスイッチングハブ304における伝送速度制限機構は、データ流入制御により実現できる。すなわち、ルータ（あるいは、スイッチングハブ）の入力データキューにおいて優先度の高いデータと低いデータを比較して、優先度の高いデータを優先して出力することにより実現できる。この優先制御方式に用いるバッファ制御ルールとしては、ラウンドロビン方式、流体フェアスケジューリング方式、重み付けフェアスケジューリング方式自己同期フェアスケジューリング方式WFFQ方式、仮想時計スケジューリング方式、クラス別スケジューリング方式などがある。これらのスケジューリング方式に関する情報は、戸田巌著、「ネットワークQoS技術」、平成13年5月25日（第1版）、オーム社刊の第12章などに記述されている。

[0074] （実施の形態1）

まず、本発明の実施の形態1について説明する。図9は、本実施の形態におけるパケット送受信部401の構成を示すブロック図である。このパケット送受信部401は、図5に示されたパケット送信機器101が備えるパケット送信部とルータ102が備えるパケット受信部とを同時に示した仮想的な機能ブロックであるし、パケットの送受信機能を備える1台のパケット送受信部を示す機能ブロック図でもあり得る（以下、全ての実施の形態におけるパケット送受信部について同じ）。

[0075] このパケット送受信部401は、AKEを用いた暗号化によるパケット送受信を行う装置であり、AKE部402、パケット化部403、送信条件設定管理部404、パケット受信部405、暗号化データ生成部406、暗号化データ復号部407、受信条件設定管理部408、フレーム化部409およびフレーム受信部410を備える。以下、伝送手順に従

って、各構成要素の機能を説明する。

[0076] 送信条件設定管理部404は、AVデータ(送信データ)が入力される端子を示す入力端子情報、AVデータのデータフォーマットを示すデータフォーマット情報及びAVデータの属性を示す属性情報を含むAVデータ情報、具体的には、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報(ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信部(ローカル)と受信部(リモート)における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータを取得し、パケット化部403やフレーム化部409におけるヘッダやペイロードデータなどの生成を制御(パラメータの設定等を)する。

[0077] なお、パケット送受信部401におけるAVデータ(送信データ)が入力される端子を示す入力端子情報とは、例えば取り扱う信号がAVデータがMPEG—TS信号の場合、(1)デジタル放送の入力端子(日本の場合、地上デジタル放送、BSデジタル放送、110度広帯域CSデジタル放送に対応するRF入力端子がある)、(2)IEEE1394 D—I/F、(3)USB—I/F、(4)IP—I/F(Ethernet(登録商標)や無線LANの区別)、(5)アナログ映像音声入力(この場合は、パケット送受信部401内で入力されたアナログ映像音声をMPEG—TS信号に変換する)などがある。なお、デジタル放送に関しては、映像情報メディア学会誌、Vol. 58、nO. 5、pp. 604ーpp. 654において解説記事がある。

[0078] また、パケット送受信部401におけるAVデータのデータフォーマットを示すデータフォーマット情報とは、例えば取り扱う信号がAVデータがMPEG—TS信号の場合、MPEG—TSのMIME—Typeやメディアフォーマットを表わす。たとえば、送信手段(サーバ)や受信手段(クライアント)が取り扱う静止画メディア、音楽メディア、動画メディアに対して、それぞれのメディアフォーマットを定める。静止画のメディアフォーマットとしては、JPEG、PNG、GIF、TIFFなどがある。また、音楽のメディアフォーマットとしては、リニアPCM、AAC、AC3、ATRAC3plus、MP3、WMAなどがある。また、動画(映像)のメディアフォーマットとしては、MPEG2、MPEG1、MPEG4、WMVなどがある。これらは、たとえば、DLNA(Digital Living Network Alliance

；ホームページはwww. dlna. org)でも同様に規定されている。DLNAのversion 1. 0では、サーバ(コンテンツの送信側、DTCPではソース)をDMP(Digital Media Server)、クライアント(コンテンツの受信側、DTCPではシンク)をDMP(Digital Media Player)と呼んでいる。DMSはUPnP—AVのMediaServer(MS)とControlPoint(CP)により構成され、DMPはUPnP—AVのMediaRenderer(MR)とControlPoint(CP)により構成される。UPnP—AVのMS, MR、CPについては、UPnPのホームページ、www／upnp. orgに記載されている。

[0079] 映像メディアフォーマットの場合、(1)解像度の区別(SD、HD)、(2)TV方式の区別(アナログではNTSC、PAL, SECAM, デジタルでは米国ATSC、欧州DVB、日本のISDBなどARIB規格に基づく放送方式)、(3)タイムスタンプ形式などの付加情報の有無、などを追加パラメータとして持つ。なお、たとえば映像の場合、MPEG—PSでもMPEG—TSに対してもMIME—Typeは"mpeg／video"であるので、上記の付加情報を用いることにより、よりきめ細かい映像メディアの取り扱い、制御が可能となる。

[0080] デジタル放送に関するARIB規格の概要は、たとえば、松下テクニカルジャーナル2004年2月、Vol. 50、No. 1、7ページから12ページで解説されている。

[0081] また、パケット送受信部401におけるAVデータの属性を示す属性情報とは、例えば取り扱う信号がAVデータが日本における地上デジタル放送システムで放送局より放送され、家庭等の受信機で選局されたMPEG—TS信号(正確には、ARIB標準規格、ARIB STD B21、第9章において、シリアルインタフェースの入出力トランスポートストリームとして規定されているパーシャルトランスポート信号)の場合、その属性情報としては、放送局よりPSI／SI情報として送信される、チャンネル名(放送局名)、チャンネル番号、番組名、番組のジャンル、スケジュールされた放送開始時間、スケジュールされた放送終了時間、番組内容に関する情報、番組の解像度、パレンタルなどの視聴制限情報、コピー制御情報、視聴料金などがある。PSIに関しては、ARIB技術資料、ARIB TR—B14やARIB TR—B15にて規定されている。

[0082] AKE部402は、認証部413と暗号化鍵交換部414を具備する。このAKE部402は、認証と鍵交換に関する設定情報(AKE設定情報)を取得し、このAKE設定情報

に関連した情報、たとえば、コピー保護情報と暗号化鍵変更情報をパケット化部403に出力する。

[0083] パケット化部403(403a)は、送信条件設定管理部404から送られてくる送信パラメータに従って、AKE部402から送られてくるAKE設定情報に関連した情報をTCP/IPのヘッダとして付加し、フレーム化部409に送る。

[0084] フレーム化部409は、送信条件設定管理部404から送られてくる送信パラメータに従って、パケット化部403からのIPパケットに対してさらにMACヘッダを付加することで、イーサネット(登録商標)フレームに変換し、送信フレームとしてネットワークに出力する。

[0085] 受信側では、フレーム受信部410は、ネットワークより入力される信号(フレーム)に対して、MACヘッダを元にフィルタリングして受信し、IPパケットとしてパケット受信部405に渡す。

[0086] パケット受信部405(405a)は、フレーム受信部410から送られてくるIPパケットに対して、IPパケットヘッダなどの識別によりフィルタリングを行い、AKE部402に出力する。これにより、送信側のAKE部と、受信側のAKE部がネットワークを介して接続されるので、通信プロトコルを介してお互いにメッセージの交換ができる。すなわち、AKE部の設定手順に従い、認証と鍵交換が行われる。

[0087] 送信側と、受信側で認証と鍵交換が成立すれば、暗号化したAVデータを送信する。

送信側では、MPEG—TS信号が暗号化データ生成部406に入力され、暗号化データ生成部406内の暗号化部411は、MPEG—TS信号を暗号化する。続いて、暗号化情報ヘッダ付加部412は、AKE部402からお鞍手くる前述したEMIおよびシード情報(シード情報のすべてのビット、または、O/Eなど一部のビット)などのAKE情報を暗号化情報ヘッダとして付加し、パケット化部403に出力する。パケット化部403は、暗号化データ生成部406からのデータに対して、送信条件設定管理部404からの送信条件などのパラメータを用いて、TCP/IPのヘッダを付加し、フレーム化部409に送る。フレーム化部409は、パケット化部403からのIPパケットに対して、802.1Q(VLAN)方式を用いてMACヘッダを付加することでイーサネット(登録商標)フ

レームに変換し、送信フレームとしてネットワークに出力する。ここで、MACヘッダ内のTCI(Tag Controal Informaition)内のPriority(ユーザ優先度)を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。

[0088] 受信側では、ネットワークより入力される信号がフレーム受信部410でMACヘッダを元にフィルタリングされ、IPパケットとしてパケット受信部405に入力される。パケット受信部405でパケットヘッダなどの識別によりフィルタリングされ、暗号化データ復号部407に入力され、暗号化データ復号部407にて暗号化情報ヘッダの除去と暗号の復号化が行われ、復号されたMPEG—TS信号が出力される。

[0089] なお、送信条件設定管理部404には、受信条件設定管理部408を介して、受信状況を送信側にフィードバックするためのデータが入力され、送信条件設定管理部404において、IPパケットのパケット化部403およびイーサネット(登録商標)フレームのフレーム化部409で生成するヘッダおよびペイロードデータが設定される。

[0090] 次に、図10のプロトコルスタックを用いて上記手順を補足説明する。図10に示された送信側において、まず送信側から受信側へ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。受信側は、コンテンツのコピー保護情報の解析を行い、認証方式を決定し、認証要求をパケット送信機器に送る。次に、乱数を発生させ、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力し、認証鍵を生成する。受信側でも所定の処理により認証鍵の共有を図る。なお、ここで用いる暗号化情報としては、たとえば、送信側の独自情報(機器ID、機器の認証情報、マックアドレスなど)、秘密鍵、公開鍵、外部から与えられた情報などを1つ以上組み合わせて生成した情報であり、DES方式やAES方式など暗号化強度の強い暗号化方式を用いることにより強固な暗号化が可能である。そして、送信側は認証鍵を用いて交換鍵を暗号化して受信側に送り、受信側で交換鍵が復号される。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵を生成する。なお、送信側では暗号鍵を時間的に変化させるために、時間的に変化する鍵更新報を生成し、受信側に送信する。コンテンツであるMPEG—TSは暗号化鍵により暗号化される。そして暗号化されたMPEG—TSは、AVデータとしてTCP(またはUDP)パケットのペイロードとしてTCPパケットが生成される。さらにこのTCPパケットはIP

パケットのデータペイロードとして使用され、IPパケットが生成される。さらにこのIPパケットはMACフレームのペイロードデータとして使用され、イーサネット(登録商標)MACフレームが生成される。なお、MACとしてはイーサネット(登録商標)であるIEEE802．3だけでなく、無線LAN規格のIEEE802．11のMACにも適用できる。

[0091] さて、イーサネット(登録商標)MACフレームは、イーサネット(登録商標)上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット(登録商標)MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからTCP(またはUDP)パケットが抜き出される。そして、TCP(またはUDP)パケットからAVデータが抜き出され、交換鍵と鍵変更情報より復元された復号鍵により、MPEG―TS(コンテンツ)が復号され出力される。

[0092] 以上のように、本実施の形態によれば、MPEG―TS信号などのAVストリームをパケット送信機器で暗号化して、IPパケットをネットワークにより伝送し、パケット受信機器で元の信号に復号することが可能である。

[0093] なお、図8において、スイッチングハブを用いたネットワークトポロジーを工夫することにより、ストリーム伝送とファイル転送を共存させることができる。たとえば、1階と2階の間のネットワーク305の帯域を、従来の技術で説明した100Mbpsから1Gbpsに拡張することによって、1階と2階のPC間でのファイル転送をバックグラウンドで行いながら、同時に、1階および2階のDVDレコーダ、PC、TVの間でMPEG―TSを暗号化してリアルタイムで伝送することができる。たとえば、市販されている100Mbpsのポートを8つ、1Gbpsのポートを1つ持ったスイッチングハブを用い、1階と2階を結ぶネットワーク305に1Gbpsのポートを接続し、残りの8chの100Mbpsのポートに TVなどのAV機器を接続する。100Mbpsのポートは8つなので、8つのポートのデータがそれぞれ最大100Mbpsで入力されて1Gbpsのポートに出力されたとしても、100Mbps×8ch＝800Mbpsと1Gbpsより小さいため、8つのポートから入力されたデータはスイッチングハブ内部で失われず全て1Gbpsのポートに出力される。よって、1階で発生したデータは全て2階に伝送することが可能である。また、逆に2階で発生したデータも全て1階に伝送することが可能である。以上のように、スイッチングハブを用いる場合、ネットワークトポロジーを工夫することによりストリーム伝送とファイル転送を

共存させることができる。

[0094] （実施の形態2）

次に、本発明の実施の形態2について説明する。図11は、本実施の形態におけるパケット送受信部401aの構成を示すブロック図である。図11においては、認証モード決定部601以外は、図9に示されたパケット送受信部401と同様の構成である。よって以下では新規な部分について説明する。

[0095] 図11において、AKE部402に対してAKE設定情報として、認証用のTCPのポート番号が、本図に示されるように、管理制御データとして、送信条件設定管理部404に入力される。ここで、認証用のTCPポート情報は、コンテンツ毎または放送チャネル毎にアクセス位置を指定するURI、または、Queryにより拡張されたURI情報とにより与える。このとき、URIについて、主データ部にコンテンツのURI情報、Query部にそのコンテンツの認証情報をマッピングする。これにより、もし、Query部がなければそのコンテンツの伝送には認証が不必要であり、Query部が存在すればそのコンテンツの伝送には認証が必要である様にモード設定することができる。URIとQueryの例は、例えば下記の形式で与えることができる。

[0096] ＜service＞:／／＜host＞:＜port＞／＜path＞／
＜filename＞.＜ext＞？AKEPORT＝＜port2＞

ここで、＜host＞:＜port＞／＜path＞／＜filename＞.＜ext＞はAVコンテンツのURIとファイル名称を表しており、？以下のQuery部における＜port2＞は認証用ポート番号を表している。ただし、認証用ポートのIPアドレスはAVコンテンツのIPアドレスと同じ場合である。

[0097] 送信側はこのURIとQueryで認証の実行モード情報を受信側に与える。受信側はWEBブラウザやUPnP−AVのCDS（Content Directory service）を用いて、上記のURIとQuery情報を受け取り、認証モード決定部601が認証モードを決定することができる。その他の動作は、実施の形態1と同様である。

[0098] （実施の形態3）

次に、本発明の実施の形態3について説明する。図12は、本実施の形態におけるパケット送受信部401bの構成を示すブロック図である。図12においては、送信条件

設定管理部404に入力されるAVデータの入力ソース情報（放送、蓄積）以外は、図11に示される実施の形態2のパケット送受信部401aと同様の構成である。よって以下では新規な部分について説明する。

[0099] 送信条件設定管理部404は、入力されたAVデータの入力ソース情報（放送、蓄積）に対して、必要データを抽出され、暗号化データ生成部406に出力される。そして、暗号化データ生成部406内の暗号化情報ヘッダ付加部412は、送信条件設定管理部404から送られてきた必要データを、以下の様に、暗号化情報ヘッダとして付加する。

[0100] 送信条件設定管理部404に入力されるAVデータの入力ソース情報（放送、蓄積）としては、たとえば次のケースが考えられる。

（ケース1）AVデータがコピーフリーコンテンツを放送する放送チャネルで受信されるコンテンツである場合。この様な放送チャネルの例としては、たとえば、アナログ放送であるVHF、UHF、またはBSアナログ放送の放送チャネルがある。

（ケース2）AVデータが一定期間でもコピーフリーでないコンテンツを放送する放送チャネルで受信されるコンテンツの場合。この様な放送チャネルの例としては、たとえば、BSデジタル放送の有料チャネルやCATV放送による有料チャネルがある。この一定期間でもコピーフリーでないコンテンツを放送する放送チャネルのコピー制御情報は、コピーネバー、コピーワンジェネレーション、およびEPN（Encryption Plus Non—assetion）フラグ付きコピーフリーが放送内容により時々刻々と切り替わるのが特徴である。

[0101] ここで、一定期間でもコピーフリーでないコンテンツを放送する放送チャネルの受信は、放送の配信を行う事業者との間での認証部により正当な受信装置または受信ユーザであることを認証された場合に行われるように制御できる。この認証の例としては、日本のデジタル衛星放送のB—CAS（BS—Conditional Access Systems）カード、または米国のCATV放送で使用されるPODカードなどのセキュリティモジュールによる認証が考えられる。

[0102] また、暗号化情報ヘッダの付加制御は、たとえば以下の様に行なう。すなわち、コピーフリーコンテンツを放送する放送チャネルを受信した場合には付加しない。また、

一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信した場合には付加する。さらに、AVデータが蓄積メディアよりコピーフリータイトルのコンテンツを再生した場合には付加しない。そして、AVデータが蓄積メディアよりコピーフリーでないタイトルのコンテンツを再生した場合には付加する。

[0103] 以上のように、暗号化情報ヘッダの付加制御を行うことにより、著作権者が設定したAVコンテンツのCCI(コピー制御情報)をネットワーク伝送においても継承して伝えていくことができる。さらに、送信側と受信側で暗号化情報ヘッダの付加制御のルールを揃えることにより異機種間での動作互換性を確保することができる。

[0104] (実施の形態4)

次に、本発明の実施の形態4について説明する。図13は、本実施の形態におけるパケット送受信部401cの構成を示すブロック図である。図13においては、送信キュー制御部801、第1キュー802、および第2キュー803以外は、図9に示された実施の形態1のパケット送受信部401と同様の構成である、よって以下では新規な部分について説明する。

[0105] AKE部402に対してAKE設定情報が入力され、このAKE設定情報に関連した情報(たとえば、コピー保護情報と暗号化鍵変更情報)、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報(ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信部(ローカル)と受信部(リモート)における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが、送信条件設定管理部404からパケット化部403に入力され、パケット化部403においてTCP/IP処理が行われ、第1キュー802に入力される。また、送信側ではMPEG-TS信号が暗号化データ生成部406に入力され、暗号化データ生成部406においてMPEG-TS信号が暗号化された後、この暗号化されたMPEG-TS信号がパケット化部403に入力され、パケット化部403においてTCP/IP処理が行われ、第2キュー803に入力される。

[0106] 送信キュー制御部801は、第1キュー802と第2キュー803にデータが存在する場合、どちらのデータを優先して出力するかの制御を行なう。通常状態では、一般データよりもMPEG-TSなどのコンテンツデータを優先制御して出力する。たとえば、パ

ケット送受信機器間でMPEG—TSを低レイテンシ(低遅延)で伝送する場合には、MPEG—TS用バッファも小さくなるため、オーバーフローが発生しやすい。送信側でMPEG—TSバッファがオーバーフローしそうになった場合、あるいは、受信側からフィードバックされた情報を参照して受信側のMPEG—TSのバッファがアンダーフローしそうになったことが判明した場合には、MPEG—TSデータを優先出力する様に第2キュー803の優先度を更に適応的に上げることにより、これらバッファ破綻を回避できる。

[0107] ただし、受信側機器(リモート機器)の再生、停止などの機器制御応答をより速くするには、第1キュー802の優先度を適応的に上げればよいが、これでは前述したMPEG—TSバッファのオーバーフローまたはアンダーフローが発生する可能性がある。

[0108] バッファのオーバーフローやアンダーフローを避け、かつ、受信側機器(リモート機器)の再生、停止などの機器制御応答をより速くする別の方法として、機器制御用パケットだけは、第1キュー802および第2キュー803キューを経由せずに、直接、フレーム化部409に出力することにより、迅速な制御応答が実現される。あるいは、機器制御用パケットに対して第3キューを新たに用意する方法により、迅速な制御応答が実現される。なお、受信側の動作は実施の形態1と同様である。

[0109] (実施の形態5)

次に、本発明の実施の形態5について説明する。図14は、本実施の形態におけるパケット送受信部401dの構成を示すブロック図である。図14においては、パケット化部403内の第1パケット化部901および第2パケット化部902、パケット受信部405内の第1パケット受信部903および第2パケット受信部904以外は図13に示された実施の形態4のパケット送受信部401cと同様の構成である。よって以下では新規な部分について説明する。

[0110] 図14において、AKE部402に対してAKE設定情報が入力され、このAKE設定情報に関連した情報(たとえば、コピー保護情報と暗号化鍵変更情報)、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報(ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信部(ローカル)と受信部(リモート)における機器の管理制御データと、受

信状況を送信側にフィードバックするためのデータが、第1パケット化部901に入力され、パケット化部901においてプロセッサを用いたソフトウェア処理でTCP／IP処理がなされ、第1キュー802に入力される。

[0111] 送信側ではMPEG—TS信号が暗号化データ生成部406に入力され、暗号化データ生成部406においてMPEG—TS信号に暗号化された後、この暗号化されたMPEG—TS信号がパケット化部403に入力され、ハードウェア処理によりUDP／IPの処理をされ、第2キュー803に入力される。

[0112] 送信キュー制御部801は、第1キュー802と第2キュー803の双方にデータが存在する場合、前述の実施の形態2と同様に、2つのキューからのデータ出力に関して優先制御を行なう。

[0113] さて、受信側では、ネットワークより入力される信号がフレーム受信部410でMACヘッダを元にIPパケットがフィルタリングされる。ここでは、上記第1パケット化部901から出力されたIPパケットが第1パケット受信部903に入力され、上記第2パケット化部902から出力されたIPパケットがおよび第2パケット受信部904に入力される。第1パケット受信部903では、プロセッサを用いたソフトウェア処理でTCP／IPの受信処理が行われ、AKE部402または受信条件設定管理部408に出力される。また、第2パケット受信部904では、ハードウェア処理によりUDP／IPの受信処理が行われ、暗号化データ復号部407に入力され、暗号化データ復号部407において暗号が復号され、MPEG—TSが出力される。

[0114] 次に、図15のプロトコルスタックを用い、上記手順を補足説明する。図15においては、MPEG—TSなどAVデータのトランスミッション層がUDPである以外は、図10に示されるプロトコルスタックと同様である、よって以下では新規な部分について説明する。図15に示された送信側において、コンテンツであるMPEG—TSは暗号化鍵Kcにより暗号化される。そして暗号化されたMPEG—TSは、前述したEMIおよびシード情報とともにAVデータとして、ハードウェアによりUDPパケットのペイロードとしてUDPパケットが生成される。さらにこのUDPパケットはIPパケットのデータペイロードとして使用され、IPパケットが生成される。

[0115] なお、送信側から受信側へのEMIおよびシード情報の伝送方法としては、たとえば

、専用の別パケットを生成して伝送することも可能であり、これによって、暗号鍵復元がさらに困難となり、コンテンツの盗聴、漏洩がより困難化される。また、インターネットなどの公衆網において、リアルタイムに伝送されるAVデータの暗号化パラメータを変化させたり、別パケットで送ると、コンテンツの盗聴、漏洩をより困難にすることができる。管理制御データに関しては、図10の例と同様に、ソフトウェア処理によりTCPパケットが生成され、IPパケット化される。

[0116] さて、イーサネット(登録商標)MACフレームは、イーサネット(登録商標)上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット(登録商標)MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからUDPパケットが抜き出され、UDPパケットからAVデータが抜き出され、交換鍵とシード情報より復元された復号鍵Kcにより、MPEG—TS(コンテンツ)が復号され出力される。

[0117] 図16は、MPEG—TSをIPパケット化、さらにイーサネット(登録商標)フレーム化して伝送する場合のパケット形式の一例を示す。188バイトのMPEG—TSに6バイトのタイムコード(TC)を付加して194バイトの単位を作る。TCは42ビットのタイムスタンプと6ビットのベースクロックID(BCID)により構成される。BCIDによりタイムスタンプの周波数情報を表すことができる。たとえば、(ケース1)BCIDが0x00の場合は、タイムスタンプの周波数情報はない、(ケース2)BCIDが0x01の場合は、タイムスタンプの周波数情報としては27MHz(MPEG2のシステムクロック周波数)である、(ケース3)また、BCIDが0x02の場合は、タイムスタンプの周波数情報としては90kHz(MPEG1で使用されるクロック周波数)である、(ケース4)BCIDが0x03の場合は、タイムスタンプの周波数情報としては24．576MHz(IEEE1394で使用されるクロック周波数)である。(ケース5)BCIDが0x04の場合は、タイムスタンプの周波数情報としては100MHz(イーサネット(登録商標)で使用される周波数)である、という様にBCIDでタイムスタンプの周波数情報を表すことができる。194バイト単位のデータを2つあわせて暗号化して、更に14バイトの暗号化情報ヘッダと合わせてRTPのペイロードとする。ここで、暗号化情報ヘッダは、4ビットのEMIと、64ビットのシード情報と12ビットのResearved Dataにより構成される。RTPパケットはUDPおよびIPによりパケット

化された後、イーサネット(登録商標)フレーム化される。イーサネット(登録商標)ヘッダとしては、図16に示される様に、標準的なイーサネット(登録商標)ヘッダとIEEE802．1Q(VLAN)により拡張されたイーサネット(登録商標)ヘッダの両方をサポートする。なお、IEEE802．1Q(VLAN)により拡張されたイーサネット(登録商標)ヘッダにおけるTCIフィールドの中の3ビットのPriorityフラグにより、イーサネット(登録商標)フレームの優先度を設定することができる。

[0118] 以上により、パケット送受信機器間でMPEG—TS信号を暗号化してリアルタイム伝送が可能となるだけでなく、第2パケット化部902がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。これにより、全ての優先データパケットが完全に送信され、リアルタイム性の保証された高品質映像の伝送が可能となる。また、一般データは一時的にバッファ部に蓄積され、優先データ伝送が優先して行なわれる中で間欠的に伝送される。また、データ量の小さい第1パケット化部901はマイコンなど安価なプロセッサで処理できる。

[0119] さらに、ハードウェア処理により、受信処理においても、イーサネット(登録商標)フレームを受信して、OSI参照モデルにおける3層のIPヘッダ、4層のUDPヘッダを同時に検査することもできる。MPEG—TSパケットと一般データパケットを分離し、MPEG—TSパケットの処理をハードウェアで行うことにより、受信フレームの取りこぼしが発生せず、リアルタイム性が保証された高品質な受信ができる。

[0120] パケットの送信タイミング、あるいは、2つの送信データキューからのデータ送信割合を、ソフトウェアではなく、ハードウェアで制御するとクロック単位で完全な送出制御が可能である。これにより全ての優先パケットが完全に送信され、リアルタイム性の保証された高品質の伝送が可能となる。また、出力パケットのシェイピングもクロック単位で正確に行われるため、初段のルータ、またはスイッチングハブでのパケット廃棄の発生確率が非常に少ない高品質な通信が可能となる。

[0121] ここで、本実施の形態における第1の変形例について説明する。図17は、その変形例におけるパケット送受信部401eの構成を示すブロック図であり、AKE部にDTCP方式を用いた場合の一例である。また、図18(a)は、パケット化部403内の第1パケッ

ト化部901および第2パケット化部902、図18(b)は、パケット受信部405内の第1パケット受信部903および第2パケット受信部904におけるパケット処理についての説明図である。

[0122] 図17に示されるように、AKE部402内のDTCP情報生成部1201、AKEコマンド受信処理部1202、AKEコマンド送信処理部1203、交換鍵生成部1204、暗号化鍵生成部1205、暗号鍵変更情報生成部1206および復号鍵生成部1207以外は図14に示される実施の形態5のパケット送受信部401dと同様の構成である、よって以下では新規な部分について説明する。

[0123] このパケット送受信部401eは、図19のフローチャートに示されるように、以下のステップでDTCP方式により暗号化コンテンツの伝送を行なう。

(ステップS11)コピー制御情報がDTCP情報生成部1201に入力される。

(ステップS12)まず、ソース側でコンテンツの送信要求を発生させ、DTCP情報生成部1201より、コンテンツの保護モード情報(EMI情報)が第1パケット化部901に出力され、パケット化部901でパケット化された後、シンクに送信される。

(ステップS13)そして、受信側(シンク)では、第1パケット受信部903よりAKEコマンド受信処理部1202にコンテンツのコピー保護情報が入力されると、AKEコマンド受信処理部1202は、そのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、AKEコマンド送信処理部1203を通じて認証要求をソースに送る。

(ステップS14)ソースとシンク間でDTCP所定の処理が行なわれ、認証鍵が共有される。

(ステップS15)次に、ソースでは、AKE送信処理部1203は、認証鍵を用いて交換鍵を暗号化し、第1パケット化部901を経由してシンクに送る。シンクでは、AKEコマンド受信処理部1202から与えられる情報により、交換鍵生成部1204において交換鍵が復号される。

(ステップS16)ソースでは、暗号鍵を時間的に変化させるために、暗号化鍵生成部1205において、時間的に変化するシード情報(O/E)が生成され、DTCP情報生成部1201および第1パケット化部901を経由してシンクに送信される。

(ステップS17)ソースでは、暗号化鍵生成部1205において交換鍵とシード情報より暗号化鍵が生成され、暗号化データ生成部406でMPEG—TSが暗号化され、第2パケット化部902に出力される。

(ステップS18)シンクでは、暗号鍵変更情報生成部1206は、第1パケット受信部903よりシード情報を受信し、復号鍵生成部1207は、このシード情報と交換鍵生成部1204の情報より、復号鍵を復元する。

(ステップS19)シンクでは、この復号鍵を用いて暗号化データ復号部407において、暗号化されたMPEG—TS信号が復号される。

[0124] 図18(a)に示されるように、第1パケット化部901では、入力データは、RTCPまたはRTSP、TCPまたはUDP、さらにIPによる処理がなされ、出力される。なお、RTCP(rfc1889)は、ネットワークの実効帯域幅や遅延時間などを受信装置より送信装置に送り、送信装置は報告された通信状態に合わせてRTPで送信するデータの品質を調整して送信することもできる。また、RTSP(rfc2326)は、再生、停止、早送り、などの制御コマンドを送ることもでき、AVファイルよりデータをダウンロードしながらコンテンツを再生することが可能である。また、第2パケット化部902では、入力データは、RTP、UDP、そしてIPでそれぞれ処理され、IPパケットが出力される。

[0125] 一方、図18(b)に示されるように、第1パケット受信部903では、受信デーは、フィルタリングなどIP受信処理、TCPまたはUDPの受信処理、さらに、RTCPまたはRTSPによる受信処理がなされ、データが出力される。また、第2パケット受信部904では、受信データは、フィルタリングなどIP受信処理、UDPの受信処理、さらに、RTPの受信処理がなされ、データが出力される。

[0126] 以上により、パケット送受信機器間でMPEG—TS信号をDTCP方式により暗号化してリアルタイム伝送が可能となるだけでなく、第2パケット化部902がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい第1パケット化部901はマイコンなど安価なプロセッサで処理できる。

[0127] 続いて、本実施の形態における第2の変形例について説明する。この変形例に係るパケット送受信部の基本的な構成は、図17に示された第1の変形例と同様である。

ただし、図20に示されるように、パケット化部403a（より厳密には、パケット化部902a）と、パケット受信部405a（より厳密には、パケット受信部904a）が第1と変形例と異なる。つまり、図20に示されるように、図20（a）の第2パケット化部902a、および図20（b）の第2パケット受信部904a以外は図18に示された第1の変形例と同様の構成である、よって以下では新規な部分について説明する。

[0128] 第2パケット化部902aは、内部で入力データにエラー訂正処理を行ない、RTP、UDP、そしてIPでそれぞれ処理してIPパケットを出力する。

[0129] また、第2パケット受信部904aは、内部でフィルタリングなどIP受信処理、UDPの受信処理、RTPの受信処理、さらにエラー訂正復号処理を行い、エラー訂正されたデータを出力する。

[0130] 図21は、第2の変形例におけるプロトコルスタックの説明図であり、送信側では、AVデータはエラー訂正符号が付加され（ECCエンコード）、UDPに渡される。また、受信側では、UDP処理よりデータを受け取り、エラー訂正後に上位層にAVデータとして渡される。

[0131] ここで、エラー訂正処理の例を図22および図23を使用して説明する。図22は、エラー訂正方式がリードソロモン方式の場合の訂正処理を説明する図であり、図23は、エラー訂正方式がパリティの場合の訂正処理を説明する図である。MPEG—TSを2つ単位でエラー訂正インターリーブマトリックスに入力する。なお、各行にはシーケンス番号を2バイト使用する。そして、図22および図23に示されるように、たとえば前述した10バイトのDTCP情報（EMI情報4ビット、シード情報64ビット、その他12ビット）を用い、さらに、RTPヘッダ、UDPヘッダ、IPヘッダ、イーサネット（登録商標）ヘッダを付加してイーサネット（登録商標）フレームが構成される。

[0132] 以上により、パケット送受信機器間でMPEG—TS信号をDTCP方式により暗号化し、さらにエラー訂正符号を付加しリアルタイム伝送が可能となる。さらに、第2パケット化部902がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい第1パケット化部901はマイコンなど安価なプロセッサで処理できる。

[0133] （実施の形態6）

次に、本発明の実施の形態6について説明する。図24は、本実施の形態におけるパケット送受信部401fの構成を示すブロック図である。図24においては、パケット化部403b（より厳密には、第2パケット化部902b）およびパケット受信部405b（より厳密には、第2パケット受信部904b）以外は、図17に示されたパケット送受信部401eの構成と同様である。よって以下では新規な部分について説明する。

[0134] 図25は、本実施の形態におけるプロトコルスタックの説明図である。送信側では、AVデータにエラー訂正符号を付加し（ECCエンコード）、UDPに渡す場合と、HTTP経由でTCPに渡す場合とがある。ここで、AVデータをRTPに渡すかHTTPに渡すかは、受信側からの制御により、RTPまたはHTTPで行うことを切替え制御する。たとえば、AVデータのパケット化は、受信側のAVデータ出力がディスプレイ充てに出力される場合は遅延の小さいRTPを用い、受信側のAVデータ出力が記録メディアに蓄積される場合は再送によりパケット落ちを低減するHTTPを用いる。このように、切替え制御することにより受信側でディスプレイに出力する場合は低遅延でのAVコンテンツの伝送が可能となり、また、受信側で蓄積する場合はパケットロスによる信号欠落が補償された高品質なAVコンテンツの伝送が可能となる。なお、図25において、受信側のプロトコル処理は、送信側と逆の手順で処理される。

[0135] ここで、本実施の形態の第1および第2の変形例に係るパケット送受信部401gおよびパケット送受信部401hの構成を示すブロック図を、それぞれ、図26および図27に示す。これらは、それぞれ、MPEG—TSなどAVコンテンツの受信機能、または送信機能を省いた構成であり、その他は本実施の形態におけるパケット送受信部401fと同じ構成である。このようなパケット送受信部401gおよびパケット送受信部401hは、送信または受信のみの機器に対して適用可能であり、低コスト化が図れる。

[0136] （実施の形態7）

次に、本発明の実施の形態7について説明する。図28は、本実施の形態におけるパケット送受信部2401の構成を示すブロック図である。このパケット送受信部2401は、入力AVコンテンツをその関連メタ情報が持つ送信条件に従って暗号化、関連メタ情報の付加、パケット化を行う装置であり、TSストリーム識別部2402、送信条件設定管理部2403、DRM（Digital Rights Management）設定管理部2404、AK

E部2405、パケット化部2406、送信キュー制御部2407、フレーム化部2408、フレーム受信部2409、パケット受信部2410、DRMコンテンツ購入決済部2411、コンテンツバッファ2413、暗号化部2414、暗号化情報ヘッダ付加部2415、HTTP／RTPヘッダ付加部2416、条件設定部2417および復号化部2418から構成される。

[0137] ここで、送信条件設定管理部2403には、送信の対象となるAVデータが入力される端子を示す入力端子情報、AVデータのデータフォーマットを示すデータフォーマット情報及びAVデータの属性を示す属性情報を含むAVデータ情報、具体的には、送信データのフォーマット種別、送信先アドレスやポート番号などの送信情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報、送信部（ローカル）と受信部（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが入力される。

[0138] コンテンツは、その選択に関して、蓄積メディアに蓄積されたコンテンツ毎または放送チャネル毎にQueryにより拡張されたURI情報で与える。ここで、URIについて、主データ部にコンテンツのURI情報、Query部にそのコンテンツの認証情報をマッピングする。これにより、もし、Query部がなければそのコンテンツの伝送には認証が不必要であり、Query部が存在すればそのコンテンツの伝送には認証が必要である様にモード設定することができる。URIとQueryの例は、例えば下記の形式で与えることができる。

[0139] ＜service＞：／／＜host＞：＜port＞／＜path＞／＜filename＞．＜ext＞？AKEPORT＝＜port2＞

ここで、＜host＞：＜port＞／＜path＞／＜filename＞．＜ext＞はAVコンテンツのURIとファイル名称を表しており、以下のQuery部における＜port2＞は認証用ポート番号を表わす。ここで、一般に認証サーバとコンテンツ提供サーバが同一であれば、認証用ポートのIPアドレスはAVコンテンツのIPアドレスと同じであるが、認証サーバとコンテンツ提供サーバが異なる場合には認証用ポートのIPアドレスはAVコンテンツのIPアドレスと異なる。送信側はこれら、URIとQueryで認証の実行モード情報を受信側に与える。受信側はWEBブラウザやUPnP−AVのCDSを用いて、上

記のURIとQuery情報を受け取り、認証モードを決定することができる。

[0140] また、DRM設定管理部2404は、送信条件設定管理部2403またはTSストリーム識別部2402よりDRM設定情報(課金情報、再生制御情報又はコピー制御情報)を受け取り、その情報を保持、管理するとともに、AKEに必要な関連情報をAKE部2405に引き渡す。具体的には、DRM設定管理部2404は、送信条件設定管理部2403等から渡されるDRM設定情報に基づいて、AVデータの再生制御、出力制御又はコピー制御を行うための課金情報、コピー制御情報、有効期限情報、有効再生回数情報の少なくとも1つを生成し、生成した情報を認証情報としてAKE部2405に渡す。ここで、DRMは、デジタル著作権管理のことである。このDRM設定管理部2404でコンテンツ伝送にDRMの課金、購入処理が必要と判断された場合には、DRMコンテンツ購入決済部2411は、コンテンツの購入処理を行う。コンテンツの購入処理が終了後に、DRMコンテンツ購入決済部2411は、コンテンツのCCI(コピー制御情報)を設定し、AKE部2405に渡す。なお、AKE部2405は、認証処理を行う認証部と、受信側と暗号化鍵の交換を行う暗号化鍵交換部を具備する。

[0141] AKE部2405に対してAKE設定情報が入力されると、このAKE設定情報に関連した情報、たとえばコピー保護情報と暗号化鍵変更情報がパケット化部2406に入力され、パケット化部2406においてTCP/IPのヘッダを付加され、さらに、フレーム化部2408においてMACヘッダが付加され、イーサネット(登録商標)フレームに変換され、送信フレームとしてネットワークに出力される。

[0142] 図29は、本発明の実施におけるDTCP方式による暗号化コンテンツの伝送手順を示すフローチャートである。このフローチャートを用いて、DTCP方式による著作権対応のAVコンテンツの伝送ステップの一例について説明する。ここで、DRM対応のAVコンテンツとはデジタル放送のコピー制御や、サーバ型放送(ARIB規格、STD-B38)等で取り扱うRMP(Rights Management & Protection)方式や、各種のネットワークDRMで扱っているコンテンツ保護情報を表す。

[0143] ここで、RMPはTV Anytimeフォーラム(http://www.tv-anytime.org/)の提唱するシステムにおいて、コンテンツ著作権の管理や利用者プライバシーの保護を目的に策定された仕様である。また、RMPI(Rights Management & Prot

ection Information)はコンテンツ利用の条件をあらわした権利情報を記述、規定したものである。RMPIで記述できる機能としては、利用者がコンテンツを視聴できる回数、コピー可否、およびコピー回数などの利用条件である。RMPIも暗号化されてセキュアに伝送され、RMPIで保護されたコンテンツは、その記述条件の範囲内で視聴ができる。 サーバ型放送においては、受信機内のハードシスクなど蓄積デバイスにデジタル情報のままで映像の劣化無しに蓄積されたプログラムの不正利用や改ざん防止が求められている。

[0144] また、放送番組と共に伝送される放送番組に関する番組名、開始／終了時間、番組内容などのメタデータを用いて、番組を編集・再構成して視聴することが簡単になるため、放送受信者が受信した番組をどのように再生、伝送して視聴するかを制御する仕組みが重要である。

[0145] このような権利管理保護を行い一例として、秒単位で更新するスクランブル放送の暗号鍵でコンテンツを暗号化したまま受信側内のハードディスクに蓄積し、再生視聴時にその暗号を復号化する。また、スクランブル鍵を、番組単位で付与するコンテンツ鍵により暗号化し、番組単位での保護も行う。このような暗号化により、蓄積番組の不正な改ざんを防止し、また、不正に番組を複製しても、コンテンツ鍵が必要となるため視聴が不可能となる。放送局は、前述したコンテンツ鍵に有効期限などの利用条件を追加することにより、受信者が蓄積した番組に対しても、視聴許可の期間などを制御することができる。

[0146] このよう再生制御機能を利用すると、放送番組を利用許諾型サービスに展開したり、課金型サービスに展開できる。例えば、有効期限が過ぎたコンテンツを視聴する場合には、放送受信者は、放送局に番組視聴の許諾を求め、放送、電話回線やインターネットにより新しい有効期限を持つコンテンツ鍵を入手して、番組を視聴できるようになる。

(ステップS21)まず、受信側で送信側より、UPnP—AV、CDSなどで与えられるコンテンツリストより受信したいコンテンツを選択し、ソース側にコンテンツの送信要求を投げる。

(ステップS22)コピー制御情報またはDRM情報を含んだデータがTSストリーム識

別部2402により抽出され、DRM設定管理部2404経由で、AKE部2405に入力される。

[0147] DTCP情報としてはAKE部2405よりコンテンツの保護モード情報（EMI情報）が暗号化情報ヘッダ付加部2415に出力され、暗号化情報ヘッダ付加部2415においてヘッダ情報として付加された後、パケット化部2406に入力される。

（ステップS23）受信側（シンク）では、パケット受信部2410よりAKEコマンド受信処理を行うAKE部2405にコンテンツのコピー保護情報が入力されると、AKE部2405は、そのコピー保護情報を解析し、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、認証要求をソースに送る。

（ステップS24）ソースとシンク間でDTCP所定の処理が行なわれ、認証鍵が共有される。このようにして、AKE部2405による認証が行われる。例えば、入力端子情報と、データフォーマット情報と、属性情報と、課金情報、コピー制御情報、有効期限情報及び有効再生回数情報より生成する認証条件とにより、受信側（シンク）との間で認証が行われる。

（ステップS25）次に、ソースはAKE部2405において、認証鍵を用いて交換鍵を暗号化してパケット化部2406を経由してシンクに送り、シンクのAKE部において交換鍵が復号される。

（ステップS26）ソースでは暗号鍵を時間的に変化させるために、AKE部2405の暗号化鍵生成部において、時間的に変化するシード情報（O／E）が生成され、AKE部2405、暗号化情報ヘッダ付加部2415、およびHTTP／RTPヘッダ付加部2416を経由してシンクに送信される。

（ステップS27）ソースでは、暗号化鍵を生成するAKE部2405において交換鍵とシード情報より暗号化鍵を生成して、暗号化部でMPEG—TSを暗号化してパケット化部2406に出力する。

（ステップS28）シンク内部の、暗号鍵変更情報を生成するAKE部2405は、パケット受信部2410よりシード情報を受信し、このシード情報と交換鍵より復号鍵を復元する。

（ステップS29）シンクでは、復号化部2418は、この復号鍵を用いて、暗号化された

MPEG－TS信号入力を復号して出力する。

[0148] ここで、DRMコンテンツがあって、そのコピー可能回数がN回（Nは2以上の整数）である場合の動作について説明する。

[0149] まず、受信端末がDRMに対応している場合には、伝送暗号状態のCCIをCOG（1世代コピー可能）またはCNM（コピーノーモア）、またはCN（コピーネバー）に設定して伝送する。ここで、暗号化伝送されるエンベデッドCCIとして「残りのコピー可能回数情報」を（N－1）回として受信側に伝え、受信側で暗号を復号した後に、DRM対応端末では残りのコピー可能回数を（N－1）回に設定する。

[0150] また、受信端末がDRMに対応していない場合には、コンテンツのDRM情報は削除してNMCのCCIを用いて受信側に伝送する。

[0151] AKE部2405は、暗号化ヘッダ情報を暗号化情報ヘッダ付加部2415に入力し、暗号化情報ヘッダ付加部2415は、以下のように、暗号化情報ヘッダ付加制御を行なう。

[0152] なお、送信条件設定管理部2403に入力されるAVデータの関連情報（放送、または蓄積コンテンツ再生の場合）として、たとえば次のような場合が考えられる。

（ケース1） 前記AVデータがコピーフリーコンテンツを放送する放送チャネルで受信されるコンテンツの場合。この様な放送チャネルの例としては、たとえば、アナログ放送であるVHF、UHF、またはBSアナログ放送の放送チャネルがある。

（ケース2） 前記AVデータが一定期間でもコピーフリーでないコンテンツを放送する放送チャネルで受信されるコンテンツの場合。この様な放送チャネルの例としては、たとえば、BSデジタル放送の有料チャネルやCATV放送による有料チャネルがある。この一定期間でもコピーフリーでないコンテンツを放送する放送チャネルのコピー制御情報は、コピーネバー、コピーワンジェネレーション、およびEPNフラグ付きコピーフリーが放送内容により時々刻々と切り替わるのが特徴である。

[0153] ここで、一定期間でもコピーフリーでないコンテンツを放送する放送チャネルの受信は、前記放送の配信を行う事業者との間での認証部により正当な受信装置または受信ユーザであることを認証された場合に行われるように制御できる。この認証の例としては、日本のデジタル衛星放送のB－CASカード、または米国のCATV放送で使用

されるPODカードなどのセキュリティモジュールによる認証が考えられる。

[0154] また、暗号化情報ヘッダの付加制御は、たとえば以下の様に行なう。すなわち、コピーフリーコンテンツを放送する放送チャネルを受信した場合には付加しない。また、一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信した場合には付加する。さらに、AVデータが蓄積メディアよりコピーフリータイトルのコンテンツを再生した場合には付加しない。そして、AVデータが蓄積メディアよりコピーフリーでないタイトルのコンテンツを再生した場合には付加する。

[0155] 以上のように、暗号化情報ヘッダの付加制御を行うことにより、著作権者が設定したAVコンテンツのCCI(コピー制御情報)をネットワーク伝送においても継承して伝えていくことができる。さらに、送信側と受信側で暗号化情報ヘッダの付加制御のルールを揃えることにより異機種間での動作互換性を確保することができる。

[0156] ここで、パケット化部2406は、送信条件設定管理部2403により決定された送信パラメータにより、入力データのパケット化および送信を行なう。

[0157] 送信条件設定管理部2403は、送信キュー制御部2407に、送信先アドレスやポート番号などの送信情報、送信に用いるパス情報(ルーティング情報)、送信データの帯域、送信データの送信優先度などの送信条件を与える。

[0158] これらのデータは、TCP/IP処理によるパケット化部2406およびフレーム化部2408で生成するヘッダやペイロードデータなどを設定する。

[0159] 受信側では、ネットワークより入力する信号がフレーム受信部2409でMACヘッダを元にフィルタリングされ、IPパケットとしてパケット受信部2410に入力される。パケット受信部2410は、IPパケットヘッダなどの識別によりフィルタリングを行い、AKE部2405に出力する。これにより送信側のAKE部と、受信側のAKE部がネットワークを介して接続されるので、通信プロトコルを介してお互いにメッセージが交換される。すなわち、AKE部の設定手順に従い、認証と鍵交換を実行することができる。

[0160] 送信側と、受信側で認証と鍵交換が成立すれば、暗号化したAVデータを送信する。

送信側では、入力信号が例えばMPEGのフルTSストリームの場合、そのフルTSストリームをTSストリーム識別部2402に入力し、フルTSストリームをパーシャルTSスト

リームに変換する。

[0161] そして、変換されたパーシャルTSストリームをコンテンツバッファ2413に送り暗号化タイミングの調整を行う。

[0162] コンテンツバッファ2413のパーシャルTS出力を暗号化部2414に入力し暗号化を行ない、前述したEMIおよびシード情報(シード情報のすべてのビット、または、O／Eなど一部のビット)などのAKE情報を暗号化情報ヘッダ付加部2415で付加する。

[0163] さらに、この信号をパケット化部2406に入力し、送信キュー制御部2407より与えられる条件を用いてTCP／IPのヘッダを付加する。パケットの優先伝送制御を行うためには、フレーム化部2408において、たとえば、802．1Q(VLAN)方式を用いて、MACヘッダを付加しイーサネット(登録商標)フレームに変換して、送信フレームとしてネットワークに出力する。ここで、MACヘッダ内のTCI(Tag Control Information)内のPriority(ユーザ優先度)を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。

[0164] 受信側では、ネットワークより入力する信号がフレーム受信部2409でMACヘッダを元にフィルタリングされ、IPパケットとしてパケット受信部2410)入力される。パケット受信部2410はパケットヘッダなどの識別によりフィルタリングし、送信条件などの伝送関連データを条件設定部2417に出力し、AKE関連データをAKE部2405に出力し、AVコンテンツを復号化部2418に出力する。復号化部2418は、暗号化情報ヘッダの除去と暗号の復号化を行い、復号したMPEG－TS信号を出力する。

[0165] なお、条件設定部2417には、受信状況を送信側にフィードバックするためのデータが入力され、IPパケットのパケット化部2406およびイーサネット(登録商標)フレームのフレーム化部2408で生成するヘッダおよびペイロードデータを設定する情報が送信条件設定管理部2403にフィードバックされる。

[0166] 次に、図30のプロトコルスタックを用い上記手順を補足説明する。図30の送信側において、まず送信側から受信側へ暗号化されたコンテンツおよびDRM設定管理部2404より与えられるコンテンツの保護モード情報が送信される。受信側は、コンテンツのコピー保護情報の解析を行い、認証方式を決定し、認証要求をパケット送信機器に送る。次に、乱数を発生させ、この乱数を所定の関数に入力し、交換鍵を作成する

。交換鍵の情報を所定の関数に入力し、認証鍵を生成する。受信側でも所定の処理により認証鍵の共有を図る。なお、ここで用いる暗号化情報としては、たとえば、送信側の独自情報（機器ID、機器の認証情報、マックアドレスなど）、秘密鍵、公開鍵、外部から与えられた情報などを1つ以上組み合わせて生成した情報であり、DES方式やAES方式など暗号化強度の強い暗号化方式を用いることにより強固な暗号化が可能である。そして、送信側は認証鍵を用いて交換鍵を暗号化して受信側に送り、受信側で交換鍵が復号される。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵を生成する。なお、送信側では暗号鍵を時間的に変化させるために、時間的に変化する鍵更新報を生成し、受信側に送信する。コンテンツであるMPEG—TSは暗号化鍵により暗号化される。そして暗号化されたMPEG—TSは、AVデータとしてTCP（またはUDP）パケットのペイロードとしてTCPパケットが生成される。さらにこのTCPパケットはIPパケットのデータペイロードとして使用され、IPパケットが生成される。さらにこのIPパケットはMACフレームのペイロードデータとして使用され、イーサネット（登録商標）MACフレームが生成される。なお、MACとしてはイーサネット（登録商標）であるIEEE802．3だけでなく、無線LAN規格のIEEE802．11のMACにも適用できる。

[0167] さて、イーサネット（登録商標）MACフレームは、イーサネット（登録商標）上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵が生成される。そして、受信したイーサネット（登録商標）MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからTCP（またはUDP）パケットが抜き出される。そして、TCP（またはUDP）パケットからAVデータが抜き出され、交換鍵と鍵変更情報より復元された復号鍵により、MPEG—TS（コンテンツ）が復号され出力される。

[0168] 以上、MPEG—TS信号などのAVストリームがパケット送信機器で暗号化され、IPパケットでネットワークにより伝送され、パケット受信機器で元の信号に復号される。

[0169] なお、送信キュー制御部2407は、第1キューとしてのAVデータキュー、および、第2キューとしての一般データキューを具備している。

[0170] 図28に示されるように、AKE部2405に対してAKE設定情報が入力され、このAKE設定情報に関連した情報（たとえば、コピー保護情報と暗号化鍵変更情報）、およ

び、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信部（ローカル）と受信部（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータがパケット化部2406に入力され、パケット化部2406においてTCP／IP処理がなされ、第1キューに入力される。

[0171] また、送信側では、MPEG—TS信号が暗号化部2414に入力され、MPEG—TS信号が暗号化された後、この暗号化されたMPEG—TS信号がパケット化部2406に入力され、パケット化部2406においてTCP／IP処理がなされ、AVデータキューに出力される。

[0172] 送信キュー制御部2407は、第1キューと第2キューにデータが存在する場合、どちらのデータを優先して出力するかの制御を行なう。通常状態では、一般データよりもMPEG—TSなどのコンテンツデータを優先制御して出力する。たとえば、パケット送受信機器間でMPEG—TSを低レイテンシ（低遅延）で伝送する場合には、MPEG—TS用バッファも小さくなるため、オーバーフローが発生しやすい。送信側でMPEG—TSバッファがオーバーフローしそうになった場合、あるいは、受信側からフィードバックされた情報を参照して受信側のMPEG—TSのバッファがアンダーフローしそうになったことが判明した場合には、MPEG—TSデータを優先出力する様に第2キューの優先度を更に適応的に上げることにより、これらバッファ破綻を回避できる。

[0173] ただし、受信側機器（リモート機器）の再生、停止などの機器制御応答をより速くするには、第1キューの優先度を適応的に上げればよいが、これでは前述したMPEG—TSバッファのオーバーフローまたはアンダーフローが発生する可能性がある。

[0174] バッファのオーバーフローやアンダーフローを避け、かつ、受信側機器（リモート機器）の再生、停止などの機器制御応答をより速くする方法として、機器制御用パケットだけはキューを経由せずに直接フレーム化部に出力することにより、迅速な制御応答が実現される。あるいは、機器制御用パケットに対して第3キューを新たに用意する方法により、迅速な制御応答が実現される。

[0175] また、図28のAKE部2405に対してAKE設定情報が入力され、このAKE設定情

報に関連した情報（たとえば、コピー保護情報と暗号化鍵変更情報）、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信部（ローカル）と受信部（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータがパケット化部2406に入力されプロセッサを用いた内部のソフトウェア処理でTCP／IP処理をされ、一般データキューに入力される。

[0176] 送信側ではMPEG—TS信号が暗号化部2414に入力され、MPEG—TS信号が暗号化された後、この暗号化されたMPEG—TS信号がパケット化部2406に入力され、内部のハードウェア処理によりUDP／IPの処理をされ、AVデータキューに入力される。

[0177] 送信キュー制御部2407は、第1キューであるAVデータキューと第2キューである一般データキューの双方にデータが存在する場合、前述の実施の形態7と同様に、2つのキューからのデータ出力に関して優先制御を行なう。

[0178] さて、受信側では、ネットワークより入力する信号がフレーム受信部2409でMACヘッダを元にIPパケットがフィルタリングされる。ここでは、ソースの上記パケット化部2406出力されたIPパケットが、シンクのパケット受信部2410に入力される。一般データキューで受信されたパケットは、プロセッサを用いたソフトウェア処理でTCP／IPの受信処理が行われ、AKE部2405または条件設定部2417に出力される。また、AVデータキューで受信したパケットは、ハードウェア処理によりUDP／IPの受信処理が行われ、暗号化されたAVデータは復号化部2418に入力され、暗号復号を行った後にMPEG—TSが出力される。

[0179] なお、送信側から受信側への、EMIおよびシード情報の伝送方法としては、たとえば、専用の別パケットを生成して伝送することも可能であり、暗号鍵復元がさらに困難となり、コンテンツの盗聴、漏洩をより困難にできる。インターネットなど公衆網において、リアルタイムに伝送されるAVデータの暗号化パラメータが変化させたり、別パケットで送ると、コンテンツの盗聴、漏洩をより困難にすることができる。管理制御データに関しては、ソフトウェア処理によりTCPパケットが生成され、IPパケット化される。

[0180] また、AKE部2405は、送信側と受信側との間で認証を実行する認証実行モードと認証を実行しない認証不実行モードとを持ち、暗号化部2414は、AKE部2405が認証実行モード及び認証不実行モードのいずれであっても、DRM設定管理部2404より与えられるコンテンツの保護モード情報に基づく暗号化情報ヘッダの付加を行う。

[0181] さて、イーサネット(登録商標)MACフレームは、イーサネット(登録商標)上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット(登録商標)MACフレームからIPパケットがフィルタリングされる。さらにIPパケットからUDPパケットが抜き出され、UDPパケットからAVデータが抜き出され、交換鍵とシード情報より復元された復号鍵Kcにより、MPEG−TS(コンテンツ)が復号され出力される。

[0182] 以上により、パケット送受信機器間でMPEG−TS信号を暗号化してリアルタイム伝送が可能となるだけでなく、第2のパケット化部がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。これにより、全ての優先データパケットが完全に送信され、リアルタイム性の保証された高品質映像の伝送が可能となる。また、一般データは一時的にバッファ部に蓄積され、優先データ伝送が優先して行なわれる中で間欠的に伝送される。また、データ量の小さい第1のパケット化部はマイコンなど安価なプロセッサで処理できる。

[0183] さらに、ハードウェア処理により、受信処理においても、イーサネット(登録商標)フレームを受信して、3層のIPヘッダ、4層のUDPヘッダを同時に検査することもできる。MPEG−TSパケットと一般データパケットを分離し、MPEG−TSパケットの処理をハードウェアで行うことにより、受信フレームの取りこぼしが発生せず、リアルタイム性が保証された高品質な受信ができる。

[0184] パケットの送信タイミング、あるいは2つの送信データキューからのデータ送信割合をソフトウェアではなくハードウェアで制御するとクロック単位で完全な送出制御が可能である。これにより全ての優先パケットが完全に送信され、リアルタイム性の保証された高品質の伝送が可能となる。また、出力パケットのシェイピングもクロック単位で

正確に行われるため、初段のルータ、またはスイッチングハブでのパケット廃棄の発生確率が非常に少ない高品質な通信が可能となる。

[0185] 以上により、パケット送受信機器間でMPEG－TS信号をDTCP方式により暗号化してリアルタイム伝送が可能となるだけでなく、第2のパケット化部がハードウェアで構成されているため、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい第1のパケット化部はマイコンなど安価なプロセッサで処理できる。

[0186] なお、パケット送受信部2401は、データフォーマット情報と、属性情報と、課金情報、コピー制御情報、有効期限情報及び有効再生回数情報の少なくとも1つとからなる制御認証情報を、AVデータのプログラム単位毎にアクセス位置を指定するURI情報、または、Queryにより拡張されたURI情報により、プログラムのリストとして、パケット受信装置に通知してもよい。

[0187] 同様に、パケット送受信部2401は、受信側（シンク）からプログラムリストの送信要求を受けると、データフォーマット情報と、属性情報と、課金情報、コピー制御情報、有効期限情報及び有効再生回数情報の少なくとも1つとからなる制御認証情報を、AVデータのプログラム単位毎にアクセス位置を指定するURI情報、または、Queryにより拡張されたURI情報により、プログラムのリストとして、パケット受信装置に通知してもよい。

[0188] さらに、パケット送受信部2401は、AVデータの単位プログラムのコピー制御情報がコピー制御を行わない旨を示す場合に、AVデータのデータフォーマット情報を表す第1のMIME－Typeと、AVデータに間欠的に暗号化情報ヘッダを付加したデータのデータフォーマット情報を表す第2のMIME－Typeの2つのMIME－Typeを生成し、AVデータのプログラム単位毎にアクセス位置を指定する2つの拡張URI情報をパケット受信装置に提示してもよい。Universal Plug and Play（UPnP）で規定されているresを用いて、AVデータの単位プログラム（itemに相当）各々をリソースとして論理記述できる。たとえば、UPnPのCDS（Content Directory Service）を用いる場合、受信側（クライアント）は送信側（サーバ）内で論理的なdirectory構造にマッピングされているContainerに属するitemとして特定のAVデータの単位プロ

グラムをbrowsすることにより探しだすことができる。ここで、上述した2つのMIME—Typeに対するres表現としては、resのアトリビュート(attribute)であるprotocolInfoを用いて、たとえば、protocolInfoの第3フィールドに各々のMIME—Typeを挿入することにより、利用可能なリソースとしてのresを識別することができる。

[0189] コンテンツの位置を表わすURI情報は、Universal Plug and Play(UPnP)におけるresのURI指定に使用し、前記2つのMIME—Typeは前記resのattributeであるprotocolInfoの第3フィールドに挿入することによりコンテンツの識別を行う。

[0190] たとえば、<res protocolInfo="第1フィールド":"第2フィールド":"第3フィールド":"第4フィールド">"resのURI"</res>における"第3フィールド"に異なるMIME—Typeを挿入することにより、他のフィールドが同じでも、コンテンツのリソースであるresの識別が可能となる。

[0191] なお、UPnP—AVにおけるprotocolInfoの定義としては、"第1フィールド"が伝送プロトコル、"第2フィールド"がネットワーク、"第3フィールド"がコンテンツのフォーマット、また、"第4フィールド"が付加情報である。

[0192] たとえば、"第1フィールド"が"http—get"の場合、"第2フィールド"は"*"、"第3フィールド"は"MIME—Type"、また、"第4フィールド"は"付加情報"となる。また、"第1フィールド"が"rtp"の場合、"第2フィールド"は"*"、"第3フィールド"は"RTPのペイロードタイプ"、また、"第4フィールド"は"付加情報"などとして使用できる。

[0193] protocolInfoを用いた伝送制御の場合、その第4フィールド"は"付加情報"として新たな仕様を決めることにより、よりきめ細かい伝送制御が実現できる。

[0194] また、パケット送受信部2401は、マルチキャスト伝送でパケットを伝送する場合、これら2つのresで表現された信号、すなわち、暗号化情報ヘッダが付加されたパケットと付加されていないパケットの両方を出力してもよい。この場合、受信側で受信するresを適宜選択する。

[0195] (実施の形態8)

次に、本発明の実施の形態8について説明する。本実施の形態におけるパケット送受信部の構成は、基本的には、図28に示された実施の形態7と同じである。以下、実施の形態7と同じ部分の説明は省略し、異なる部分のみを説明する。

[0196] 本実施の形態では、上記実施の形態7において、ライブで放送されているコンテンツをHTTP／RTPヘッダ付加部2416および、パケット化部2406においてHTTPのチャンク伝送方式で伝送する様に伝送プロトコルを設定する。なお、チャンク伝送方式は、HTTPで規定されている伝送方式のひとつで、受信者と送信者との間で伝送データのサイズが決定されたチャンク（かたまりの）データによる伝送をいう。

[0197] これにより、従来は、前記暗号化に関して付加するヘッダ長や伝送コンテンツ長HTTPリクエストの度に、受信側（クライアント）で計算していたが、この計算の必要がなくなり、受信側の処理を軽くできる。特に、ライブ放送を受信している場合に、伝送側および受信側の処理負荷を軽減できる。

[0198] HTTPのペイロードデータ長としては、暗号化される伝送ペイロードの暗号化情報ヘッダとTSの整数倍であり、送信側で都合のよい値に設定することができる。このチャンク伝送時にはTCPのコネックションは永続的接続モード（HTTPのversionが1．0の場合、Keep Alive設定。HTTPのversion 2．0の場合はPersistent connection）されていると、TCPコネクションの切断、確立をコンテンンツ伝送中にTCPトランザクション毎に頻繁に行う必要がなくなり効率のよいAV伝送を行うことができる。よって、パケット送受信部は、AVデータの伝送プロトコルとして、TCPと決定された場合は、TCPコネクションを永続的接続にしてAVデータの伝送を効率的に安定して実現できる。

[0199] （実施の形態9）

次に、本発明の実施の形態9について説明する。図31は、本実施の形態におけるパケット送受信部2401aの構成を示すブロック図である。このパケット送受信部2401aは、図28に示された実施の形態7のパケット送受信部2401の構成に加えて、蓄積部2701を備える。以下、実施の形態7と同じ部分の説明は省略し、異なる部分のみを説明する。

[0200] このパケット送受信部2401aは、TSストリーム識別部2402に接続された蓄積部2701を具備する。ここで、蓄積部2701は、ハードディスクや光ディスクである。本実施の形態において、このパケット送受信部2401aは、ハードディスクや光ディスクなどに蓄積されたMPEG―TSデータをHTTPのレンジリクエストを用いて伝送する。

[0201] このレンジリクエストは、蓄積部2701に蓄積されたMPEG—TSファイルとペアになっているファイル中におけるIフレーム位置情報を含んだファイルである。例えば、DVD—VR方式ではIFOファイルと呼ばれているものである。このIFOファイルと同等のIフレーム位置情報を持ってファイルを用いることにより、早送り、巻き戻し、スロー再生などの特殊再生を効率よく簡単に実現できる。

[0202] 本発明で用いる入力データの適用範囲として、サーバ型放送や各社の異なるDRM方式など一般のDRM対応のAVコンテンツをDTCP—IPを用いて伝送することが可能となる。

[0203] なお、HTTPによる伝送とRTPによる伝送を切り替えてAVデータを伝送してもよい。そのとき、HTTPによる伝送として、ソースからの出力がライブ放送の受信信号またはライブ放送の受信チャネルの切り替えまたは蓄積されたプログラム選択時の再生信号の場合には、チャンク伝送を行い、プログラム選択後の蓄積メディアから再生されたプログラムからの再生信号の場合には、レンジリクエストを用いて再生を切替えて行っても実現できる。

[0204] (実施の形態10)

次に、本発明の実施の形態10について説明する。図32は、本実施の形態におけるパケット送受信部2401bの構成を示すブロック図である。このパケット送受信部2401bは、図31に示された実施の形態9のパケット送受信部2401aの構成に加えて、Iフレーム位置情報生成部2801を備える。以下、実施の形態9と同じ部分の説明は省略し、異なる部分のみを説明する。

[0205] 蓄積部2701において、ハードディスクや光ディスクなどに蓄積された異なる蓄積フォーマットのコンテンツの場合、クライアント(シンク)は全ての異なるコンテンツのIフレーム位置データを格納したファイルを理解しなければならない。そこで、本実施の形態では、フォーマット数が多くなると、これは受信側にとって大きな負担となるため、送信側で異なるIフレーム位置情報より、共通のIフレーム位置情報生成部2801で共通のIフレーム位置情報を生成する。これにより、各社のHDD記録フォーマット、DVD—VR方式、あるいはBD方式など異なる蓄積フォーマットであっても、簡単に、早送り、巻き戻し、スロー再生などの特殊再生することが実現される。

[0206] このパケット化において、HTTPは受信部からのレンジリクエストまたはデータ取得コマンドを受けて前記AVデータまたは前記暗号化モード情報のうち少なくとも一方を含んだペイロードデータを伝送する。このレンジリクエストまたはデータ取得コマンドは、前記送信側における前記AVデータがMPEGの場合、MPEGストリームにおける不連続発生連続性情報、前記AVデータのファイル内におけるMPEGのIピクチャまたはPピクチャまたはBピクチャの位置情報、或るIピクチャから次のIピクチャの間に存在するPピクチャとBピクチャの各個数または合計個数の内、少なくとも1つの情報を参照して実行する。ここで、MPEGストリームにおける不連続発生連続性情報とは、ARIB規格、ARIB−TR−B14またはARIB−TR−B14の第2編に記載されているDIT情報を元に生成することができる。このストリームの不連続点とは、たとえば、MPEGのパーシャルTSの場合、MPEG−TSストリームのシステムタイムベースの不連続が発生する点、たとえば、PCRが不連続になる点、または、パーシャルTSを構成するパケットの内のどれか1つのトランスポートパケットヘッダのcontinuity__counterの不連続が発生する点のことである。

[0207] また、AVデータのファイル内におけるMPEGのIピクチャまたはPピクチャまたはBピクチャの位置情報は、前記AVデータが複数の異なるファーマットであった場合にもオリジナルに持っている複数のIピクチャまたはPピクチャまたはBピクチャの位置情報、前記MPEGのIピクチャまたはPピクチャまたはBピクチャの時刻情報より、複数の異なるファーマット間で共通なIピクチャまたはPピクチャまたはBピクチャ位置情報を生成し、この共通のIピクチャまたはPピクチャまたはBピクチャ位置情報を用いて前記AVデータのファイル内におけるMPEGのIピクチャまたはPピクチャまたはBピクチャの位置情報、時刻情報の参照情報とする。これにより、たとえばHDDに、異なる記録フォーマットで記録されているMPEG−TSファイルがあっても、リモート端末からは共通のIまたはPまたはBピクチャの位置情報や時間情報で特定のピクチャに直接アクセスできるという大きなメリットがある。

[0208] たとえば、図33に示される一例のように、パーシャルTSを記録したHDDやBDディスクなどから、IまたはPまたはBピクチャの連続性およびファイル内での位置情報などを統一した「ピクチャ情報ファイル」を読み出す。ネットワークを介して離れた場所に存

在する端末からは、この統一されたピクチャ情報ファイルをバイト位置や時刻情報（timestamp）で参照することにより、異なるTS記録フォーマットでも各ピクチャ位置をきめ細かに参照することができる。

[0209] 図33において、"discont"はパーシャルTSの不連続点を示す1ビットのフラグである。たとえば、この値が"0"の時はパーシャルTSは連続であり、"1"の時は不連続を意味する。また、"IPBフラグ"は、2ビットのIピクチャ、Pピクチャ、Bピクチャの識別フラグであり、その値が"00"の時はIピクチャ、"01"の時はPピクチャ、"10"の時はBピクチャであることを示す。ここで、Iピクチャの場合は必ず記述が必要で、PまたはBピクチャの場合は、オプションとし、必ずしも記述しなくてもよい。また、"Byte__position"は、Iピクチャ、Pピクチャ、およびBピクチャの先頭のファイルにおけるバイト位置を32bitで示す。さらに、"PB__number"は、或るIピクチャから次のIピクチャまでの間に存在するPピクチャとBピクチャの合計数を5ビットで示す。"Timestamp"は、Iピクチャ、Pピクチャ、Bピクチャの時刻情報で、それぞれのMPEGのIピクチャまたはPピクチャまたはBピクチャを構成するタイムスタンプ付きTS列の先頭など特定位置のTSのタイムスタンプ値を40ビットに変換して使用する。それぞれのパラメータ、フラグの値の定義は、前記の組合せに限定されない。

[0210] 以上にように、本実施の形態によれば、きめ細かやで綺麗なスロー再生や高速再生などのトリック再生が実現される。なお、このピクチャ情報ファイルはリモート端末からローカル端末内の異なるファーマットで記録されたMPEG―TSファイル内のピクチャ位置を共通のファイル形式で見せることができるフィルタ機能として考えることができる。すなわち、独自のファイル形式でMPEG―TSを記録したAVデータファイルとその関連情報ファイルより、共通のピクチャ情報ファイルを生成することができる。

[0211] また、本実施の形態により、AVコンテンツをAKEや暗号処理を実装しない送受信装置による実装の場合にも、MPEGのIピクチャまたはPピクチャまたはBピクチャに効率よくアクセスできるという効果が奏される。

[0212] さらに、本発明の別機能について説明する。コンテンツバッファ2413において、MPEG―TS信号に、たとえばリードソロモン方式のエラー訂正符号を付加した後、暗号化部2414で暗号化する。これにより、パケット送受信機器間でMPEG―TS信号をD

TCP方式により暗号化し、さらにエラー訂正符号を付加しリアルタイム伝送が可能となる。ここで、MPEG－TSのヘッダ付加および伝送処理のパケット化部をハードウェアで構成すると、本質的にソフトウェア処理に起因する送信パケットの送り残しや受信パケットの取りこぼしが発生しない。また、データ量の小さい一般データのパケット化はマイコンなど安価なプロセッサで処理できる。

[0213] なお、上述した実施の形態においては、一般のIPネットワークなどパケットの順序性が保証されていない通信網で伝送する場合には、パケットにシーケンス番号を付加して送信し、受信側でシーケンス番号を用いて順序性の保証を行ってもよい。この順序性の保証は、OSIモデルの第4層以上、すなわち、RTPやビデオ信号処理などで行なうことができる。

[0214] また、送信側でハードウェア処理され伝送されたAV信号のパケットが、ネットワークでフラグメントされないため対策ができる。すなわち、送信側において、あらかじめアプリケーションレベルの処理で、通信網においてフラグメントされない最大サイズ（MTU）を検査し、それ以下のパケットサイズで伝送すればよい。あるいは、RFCの規格では全ての端末は576バイトのサイズのIPパケットを扱えなければならないと規定されているので、ルータ等の多くのネットワーク機器はこれ以下のIPパケットではフラグメントが起こらない。したがってIPパケットのサイズが576バイト以下となるように、送信側でハードウェア処理されるAV信号のパケットサイズを調整すればよい。なお、送信側でハードウェア処理されるAV信号のパケットにフラグメントが起こらない場合は、受信したパケットがフラグメントされていれば全て一般パケットとして処理すればよい。また、イーサネット（登録商標）のIPパケットの最大値を越えた場合は送信端末でフラグメントしなければ行けないので、優先パケットのフラグメントを起こさせないためにはIPパケットの最大値以下でなければならないことは言うまでもない。

[0215] また、通信網においてフラグメントが起こる確率が非常に低い場合は、送信側でハードウェア処理され伝送されたAV信号のパケットのIPヘッダにフラグメント禁止のフラグを立てて伝送することにより、ルータがフラグメントせざるを得ない状態ではIPパケットを廃棄させることにより、受信端末のフラグメント処理負荷を軽減してもよい。この場合、非常に少数のパケットは損失となるが、受信側で誤り訂正あるいは誤り修整

を行うことで通信品質を補償することができる。

[0216] さらに、上記実施の形態では、通信網プロトコルとしてイーサネット(登録商標)を例としたが、本発明は、この限りではない。

[0217] また、ビデオ信号処理の例として、MPEG—TSを用いたが、これに限らず本発明で用いる入力データの適用範囲としては、MPEG1／2／4などMPEG—TSストリーム(ISO／IEC13818)、DV(IEC61834、IEC61883)、 SMPTE314M(DV—based)、SMPTE259M(SDI)、SMPTE305M(SDTI)、SMPTE292M(HD—SDI)等で規格化されているストリームを含んだあらゆる映像、音声に関するストリームまでも適用可能である。映像や音声のデータレートは、CBR(constant bit rate)に限るものではない。さらに、映像や音声だけでなく、一般のリアルタイムデータ、あるいは優先的に送受信を行うデータであればどのようなものでも本発明から排除するものではない。

[0218] また、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、一定の条件化でリアルタイムより高速の伝送も可能である。

[0219] また、本発明で用いる入力データの適用範囲として、サーバ型放送や各社の異なるDRM方式など一般のDRM対応のAVコンテンツをDTCP—IPを用いて伝送することが可能となる。

[0220] また、上記実施の形態において、パケット送受信装置は、Nを2以上の整数とした場合、UDPまたはTCPのN個のポートを用いて、AVデータにより構成されるN個のプログラムを前記N個のポートのそれぞれに割り当てて伝送してもよい。このとき、N個のポートのそれぞれに割り当てるN個のプログラムは、それぞれ、ソースに内蔵された放送受信チューナまたは蓄積メディアデバイスをUPnP手段のコンテナ形式で表現し、また、放送受信チャネルまたは蓄積プログラムをUPnP手段のitem形式で表現し、それぞれのitem(リソースとしてのresとなる)の存在位置をURI、また伝送プロトコルや属性情報をUPnPのprotocolInfoを用いたres表現で表わし、複数プログラムの複数クライアントへの同時伝送など、きめ細かい伝送システムを実現することができる。

[0221] また、放送受信の場合、送信側におけるN個のポートのそれぞれに割り当てるN個のプログラム(res)のソースからシンクへの伝送ストリームが複数存在する場合に、各々のストリームをUPnPのproperty形式で表わし、特定の伝送ストリームのpropertyのattributeとして、「チューナのコンテナの種別、チューナのコンテナ種別ごとのチューナID、チューナで選局されたチャネルID、伝送ストリームの他クライアントとの共有・横取りに関する利用可否情報、ストリームを伝送するトランスポート層が使用するTCPまたはRTPのポート番号、シンクにおけるUPnP−AV手段のConnectionManagerがソースにおけるConnectionManagerに対してitemに関する論理的接続に関連して設定するUPnP−AV手段のconnectionID、ソースにおけるUPnP−AV手段のConnectionManagerがシンクにおけるConnectionManagerに対してitemに関する論理的接続に関連して設定するUPnP−AVのconnectionID」のうち、いずれかを含めることにより、受信側(クライアント、シンク)から送信側(サーバ、ソース)内のチューナのチャネル選局を行なう時に、伝送ストリームのpropertyおよびそのattributeを参照することにより、伝送ストリームに空きあるか無いか、およびどのチューナの、どのチャネルが選局されているかを判別することができる。

[0222] たとえば、放送受信の場合のUPnP−AVコンテナ構造として、<root>下に、チューナーのコンテナを配置する。コンテナ種別としては、地上デジタル、BSデジタル、110度広帯域CSデジタルなどの放送システム別、各々チューナコンテナを割り当てる。この場合、各チューナーコンテナの下にitemとして各放送システムのチャンネルを割り当てる。UPnPのCDSのserchやbrowsコマンドを用いて、受信側から送信側のチューナコンテナ、およびチューナコンテナ内のチャンネルitemを認識することができる。チャンネルとしてのitemは放送局より送信される付属情報を持つ。

[0223] 同様に、蓄積コンテンツの再生の場合、送信側におけるN個のポートのそれぞれに割り当てるN個のプログラムのソースからシンクへの伝送ストリームが複数存在する場合に、UPnPのproperty形式で表わし、特定の伝送ストリームのpropertyのattributeとして、「蓄積メディアデバイスのコンテナの種別、蓄積メディアデバイスのコンテナ種別ごとの蓄積メディアデバイスID、蓄積メディアデバイスで選択されたプログラムID、伝送ストリームの共有を含む利用可否情報、ストリームを伝送するトランスポート層

が使用するTCPまたはRTPのポート番号、シンクにおけるUPnP—AV手段のConnectionManagerがソースにおけるConnectionManagerに対してitemに関する論理的接続に関連して設定するUPnP—AV手段のconnectionID、ソースにおけるUPnP—AV手段のConnectionManagerがシンクにおけるConnectionManagerに対してitemに関する論理的接続に関連して設定するUPnP—AV手段のconnectionID」のうち、いずれかを含めることにより、シンクがソース内の蓄積メディアデバイスのプログラム選択を行なう時に、伝送ストリームのpropertyおよびそのattributeを参照することにより、伝送ストリームに空きあるか無いか、およびどの蓄積メディアデバイスのどのプログラムが選択されているかなど判別することができる。

[0224] たとえば、蓄積・記録デバイスが、ハードディスクドライブ(HDD)、DVD—RAMドライブ、BDドライブの場合のUPnP—AVコンテナ構造として、<root>下に、それぞれのコンテナを配置する。コンテナ種別としては、HDD、DVD—RAMドライブ、BDドライブなどそれぞれにデバイス別のコンテナを割り当てる。この場合、各コンテナの下にitemとして、蓄積・記録コンテンツをたとえばプログラム単位で割り当てる。これにより、UPnPのCDSのserchやbrowsコマンドを用いて、受信側から送信側の蓄積・記録デバイスコンテナ、および蓄積・記録デバイスコンテナ内の蓄積・記録コンテンツをたとえばプログラム単位でitemとして認識することができる。蓄積・記録されているitemは記録時に与えられた付属情報を持つ。

[0225] また、送信サーバの放送コンテナに所属するitemをクライアントが受信して蓄積する場合、前記放送システム別のチューナコンテナの属性(地上デジタル、BSデジタル、110度広帯域CSデジタルなどの放送システムを区別する属性)を利用して、放送システム別のpropertyを生成し、蓄積・記録デバイスに蓄積・記録して生成したitemのpropertyとして保存する。これにより、蓄積・記録デバイスのコンテナが放送システム別でなくても、蓄積・記録デバイスから再生したitemのpropertyを見れば、どの放送システムから放送されたコンテンツであるかを識別することができる。

[0226] 以上により、放送受信の場合でも蓄積コンテンツの再生の場合でも、新たにサーバ接続するクライアントはサーバの使用状況を理解し、より効率的にコンテンツの選択、伝送を行うことができる。

[0227] なお、「ストリームを伝送するトランスポート層が使用するTCPまたはUDPのポート番号」、および、「シンクにおけるUPnP—AV手段のConnectionManagerがソースにおけるConnectionManagerに対してitemに関する論理的接続に関連して設定するUPnP—AV手段のconnectionID、またはソースにおけるUPnP—AV手段のConnectionManagerがシンクにおけるConnectionManagerに対してitemに関する論理的接続に関連して設定するUPnP—AV手段のconnectionID」の論理対により、UPnP—AV手段と、TCPまたはUDPを使用するHTTPまたはRTPを用いるトランスポート手段とを論理的に対応づけることにより、CDSやCMS(Connection Manager Service)を用いるUPnP—AVレイヤとHTTP／TCP／IPを取り扱うトランスポートレイヤを論理的に1対1に対応させることができるので、コネクションの確立、コンテンツの選択、コンテンツの伝送、コネクションの切断、存在コネクションの管理などの伝送制御をより簡単に実現することが可能となる。また、HTTPのリクエストメッセージのメッセージヘッダーの拡張フィールドや、HTTPのレスポンスメッセージのメッセージヘッダーの拡張フィールドにUPnP—AV手段のconnectionIDを記述することによりHTTPプロトコルによる伝送制御手段とUPnP—AV手段と論理的に1対1対応させることができる。

産業上の利用可能性

[0228] 本発明は、パケット送信装置として、例えば、デジタルチュナーやDVDレコーダ等として、特に、デジタル放送やDVDディスクのコピー制限コンテンツをコンテンツの著作権者によって設定されたコピー制御情報を継承しながらIPネットワークを用いて違法コピーを回避しつつ安全に伝送するパケット送信装置として、たとえば、一般家庭において、1階の今にあるデジタルチュナーやDVDレコーダから2階の寝室にあるディスプレイに映画などのプレミアムコンテンツを伝送するパケット送信装置として利用することができる。

請求の範囲

[1] パケット受信装置にパケットデータを送信するパケット送信装置であって、

AVデータが入力される端子を示す入力端子情報、前記AVデータのデータフォーマットを示すデータフォーマット情報及び前記AVデータの属性を示す属性情報を含むAVデータ情報を取得するAVデータ情報取得手段と、

前記AVデータ及び非AVデータの入力を受け付けるデータ入力手段と、

前記非AVデータまたは前記AVデータより、前記AVデータの課金情報、再生制御情報及びコピー制御情報の少なくとも1つの情報を抽出し、抽出した情報から、前記AVデータを送信する際の条件となる暗号化モードを示す暗号化モード情報を生成する送信条件設定管理手段と、

前記入力端子情報、前記データフォーマット情報及び前記属性情報を組み合わせて決定される送信条件に基づいて、前記データ入力手段より入力された前記AVデータを暗号化し、暗号化された前記AVデータに対して前記暗号化モード情報に基づく暗号化情報ヘッダを付加することによって暗号化データを生成する暗号化データ生成手段と、

前記暗号化データ生成手段により生成された暗号化データに対して、パケットヘッダを付加することによってパケットを生成するパケット化手段と、

前記パケット受信装置との間で認証処理を行う認証手段と、

前記入力端子情報、前記属性情報及び前記パケット受信装置より指定される送信モードを示す情報の少なくとも1つを用いて、前記パケット送信装置と前記パケット受信装置の間での前記AVデータの伝送プロトコルを決定する伝送プロトコル決定手段と、

前記認証処理によって前記パケット受信装置との認証処理が完了した後に、前記伝送プロトコル決定手段によって決定された伝送プロトコルに従って、前記パケット化手段によって生成された暗号化データを含むパケットを前記パケット受信装置に伝送する伝送手段と

を備えることを特徴とするパケット送信装置。

[2] 前記パケット送信装置はさらに、前記送信条件設定管理手段より入力される前記課

金情報、前記再生制御情報又は前記コピー制御情報に基づいて、前記AVデータの再生制御、出力制御又はコピー制御を行うための課金情報、コピー制御情報、有効期限情報、有効再生回数情報の少なくとも1つを生成し、生成した情報を認証情報として前記認証手段に通知する著作権管理手段を備え、

前記認証手段は、前記著作権管理手段から通知された認証情報に基づいて、前記パケット受信装置との間で認証処理を行うことで、前記AVデータの前記パケット受信装置における再生制御、出力制御又はコピー制御を行う

ことを特徴とする請求項1記載のパケット送信装置。

[3] 前記パケット送信装置はさらに、前記著作権管理手段による制御の下で、前記課金情報、前記再生制御情報又は前記コピー制御情報に基づいて、前記パケット受信装置との間で、著作権保護の対象となるコンテンツの購入決済を行うコンテンツ購入決済手段を備える

ことを特徴とする請求項1記載のパケット送信装置。

[4] 前記認証手段は、前記パケット送信装置と前記パケット受信装置が規定の条件を備えていることを検証することによって認証処理を実行し、認証処理後に前記パケット送信装置と前記パケット受信装置とで暗号化鍵を共有し、前記入力端子情報と、前記データフォーマット情報と、前記属性情報と、前記課金情報、前記コピー制御情報、前記有効期限情報及び前記有効再生回数情報より生成する伝送条件とにより、前記暗号化鍵を更新し、

前記暗号化データ生成手段は、前記暗号化鍵を用いて前記AVデータを暗号化する

ことを特徴とする請求項1記載のパケット送信装置。

[5] 前記暗号化データ生成手段は、前記コピー制御情報がコピー制御をする旨を示すかコピー制御をしない旨を示すかに関係なく、前記暗号化モード情報に基づく暗号化情報ヘッダの付加を行う

ことを特徴とする請求項1記載のパケット送信装置。

[6] 前記認証手段は、前記パケット送信装置と前記パケット受信装置との間で認証を実行する認証実行モードと認証を実行しない認証不実行モードとを持ち、

前記暗号化データ生成手段は、前記認証手段が前記認証実行モード及び前記認証不実行モードのいずれであっても、前記暗号化モード情報に基づく暗号化情報ヘッダの付加を行う

ことを特徴とする請求項1記載のパケット送信装置。

[7] 前記暗号化データ生成手段は、前記コピー制御情報がコピー制御をする旨を示す場合に、前記コピー制御情報を前記暗号化情報ヘッダとして付加し、前記コピー制御情報がコピー制御をしない旨を示す場合に、前記コピー制御情報を前記暗号化情報ヘッダとして付加しない

ことを特徴とする請求項6記載のパケット送信装置。

[8] 前記認証手段は、前記入力端子情報と、前記データフォーマット情報と、前記属性情報と、前記課金情報、前記コピー制御情報、前記有効期限情報及び前記有効再生回数情報より生成する認証条件とにより、前記パケット受信装置との間で認証を行う

ことを特徴とする請求項7記載のパケット送信装置。

[9] 前記パケット送信装置はさらに、前記データフォーマット情報と、前記属性情報と、前記課金情報、前記コピー制御情報、前記有効期限情報及び前記有効再生回数情報の少なくとも1つとからなる制御認証情報を、前記AVデータのプログラム単位毎にアクセス位置を指定するURI情報、または、Queryにより拡張されたURI情報により、前記プログラムのリストとして、前記パケット受信装置に通知するアクセス位置通知手段を備える

ことを特徴とする請求項8記載のパケット送信装置。

[10] 前記パケット送信装置はさらに、前記パケット受信装置からプログラムリストの送信要求を受けると、前記データフォーマット情報と、前記属性情報と、前記課金情報、前記コピー制御情報、前記有効期限情報及び前記有効再生回数情報の少なくとも1つとからなる制御認証情報を、前記AVデータのプログラム単位毎にアクセス位置を指定するURI情報、または、Queryにより拡張されたURI情報により、前記プログラムのリストとして、前記パケット受信装置に通知するアクセス位置通知手段を備える

ことを特徴とする請求項8記載のパケット送信装置。

[11] 前記パケット送信装置はさらに、前記AVデータの単位プログラムのコピー制御情報がコピー制御を行わない旨を示す場合に、前記AVデータのデータフォーマット情報を表す第1のMIME−Typeと、前記AVデータに間欠的に前記暗号化情報ヘッダを付加したデータのデータフォーマット情報を表す第2のMIME−Typeの2つのMIME−Typeを生成し、前記AVデータのプログラム単位毎にアクセス位置を指定する2つの拡張URI情報を前記パケット受信装置に提示するアクセス位置通知手段を備える

ことを特徴とする請求項8記載のパケット送信装置。

[12] 前記2つの拡張URI情報は、Universal Plug and Play(UPnP)におけるresのURI指定に使用し、前記2つのMIME−Typeは前記resのattributeであるprotocolInfoの第3フィールドに挿入することによりコンテンツの識別を行う

ことを特徴とする請求項11記載のパケット送信装置。

[13] 前記パケット送信装置はさらに、

前記パケット受信装置に送信するAVデータ及び非AVデータをそれぞれ一時的に保持する第1及び第2バッファと、

前記第1及び第2バッファのいずれかに保持されたデータが優先して前記パケット受信装置に送信されるように優先制御する優先制御手段と

を備えることを特徴とする請求項1記載のパケット送信装置。

[14] 前記優先制御手段は、前記非AVデータが前記第2バッファでオーバーフローしないことを維持しつつ、前記AVデータが前記第1バッファから優先して出力されるように、前記優先制御を行う

ことを特徴とする請求項13記載のパケット送信装置。

[15] 前記伝送手段は、前記伝送プロトコル決定手段によって前記AVデータの伝送プロトコルとして、Transmission Control Protocol(TCP)と決定された場合は、TCPコネクションを永続的接続にして前記伝送を行う

ことを特徴とする請求項1記載のパケット送信装置。

[16] 前記認証手段は、Digital Transmission Content Protection(DTCP)方式に従って、前記パケット受信装置と暗号化鍵を共有するための認証と鍵交換を行う

ことを特徴とする請求項1記載のパケット送信装置。

[17] 前記パケット化手段は、HyperText Transfer Protocol(HTTP)、TCP又はInternet Protocol(IP)に従ったパケット化を行う

ことを特徴とする請求項1記載のパケット送信装置。

[18] 前記パケット化手段は、前記HTTPに従ったパケット化を行う場合は、レンジリクエストまたはデータ取得コマンドにより前記パケット化を行い、前記送信側における前記AVデータがMPEGの場合には、MPEGストリームにおける不連続発生連続性情報、前記AVデータのファイル内におけるMPEGのIピクチャまたはPピクチャまたはBピクチャの位置情報、前記MPEGのIピクチャまたはPピクチャまたはBピクチャの時刻情報、或るIピクチャから次のIピクチャの間に存在するPピクチャとBピクチャの各個数または合計個数のうち少なくとも1つの情報を参照して前記パケット化を行う

ことを特徴とする請求項17記載のパケット送信装置。

[19] 前記パケット化手段は、前記AVデータのファイル内におけるMPEGのIピクチャまたはPピクチャまたはBピクチャの位置情報または時刻情報として、前記AVデータが複数の異なるファーマットであった場合にもオリジナルに持っている複数のIピクチャまたはPピクチャまたはBピクチャの位置情報または時刻情報より、複数の異なるファーマット間で共通なIピクチャまたはPピクチャまたはBピクチャ位置情報または時刻情報を生成し、この共通のIピクチャまたはPピクチャまたはBピクチャ位置情報または時刻情報を用いて前記AVデータのファイル内におけるMPEGのIピクチャまたはPピクチャまたはBピクチャの位置情報または時刻情報の参照情報と前記パケット化を行う

ことを特徴とする請求項17記載のパケット送信装置。

[20] 前記パケット化手段は、HTTPに従ったパケット化を行う場合は、チャンク伝送方式で前記パケット化を行ない、HTTPパケットのペイロード長が前記パケット送信装置で決定された値となるように前記パケット化を行う

ことを特徴とする請求項17記載のパケット送信装置。

[21] 前記パケット化手段は、HTTPに従ったパケット化を行う場合は、HTTPパケットのペイロード長が、前記暗号化情報ヘッダと整数個の前記AVデータを構成するTrans

port Stream(TS)により構成されるデータの長さ、または、前記暗号化情報ヘッダと整数個のタイムスタンプつきTSにより構成されるデータの長さとなるように前記パケット化を行う

ことを特徴とする請求項17記載のパケット送信装置。

[22] 前記伝送手段は、前記HTTPによる伝送として、レンジリクエスト方式とチャンク伝送方式を切り替えて行う

ことを特徴とする請求項17記載のパケット送信装置。

[23] 前記伝送手段は、前記HTTPによる伝送として、前記パケット送信装置の出力がライブ放送の受信信号またはライブ放送の受信チャネルの切り替えまたは蓄積されたプログラム選択時の再生信号の場合には、チャンク伝送を行い、プログラム選択後の蓄積メディアから再生されたプログラムからの再生信号の場合には、レンジリクエストを用いて再生を切替えて行う

ことを特徴とする請求項17記載のパケット送信装置。

[24] 前記パケット化手段は、Real-time Transport Protocol(RTP)、User Datagram Protocol(UDP)又はIPに従ったパケット化を行う

ことを特徴とする請求項1記載のパケット送信装置。

[25] 前記伝送手段は、マルチキャスト伝送でパケットを伝送する場合、前記暗号化情報ヘッダが付加されたパケットと付加されていないパケットの両方を出力する

ことを特徴とする請求項24記載のパケット送信装置。

[26] 前記パケット送信装置はさらに、前記AVデータの単位プログラムのコピー制御情報がコピー制御を行わない旨を示す場合に、前記AVデータのデータフォーマット情報を表すc-Typeと、前記AVデータに間欠的に前記暗号化情報ヘッダを付加したデータのデータフォーマット情報を表す第2のMIME-Typeの2つのMIME-Typeを生成し、前記AVデータのプログラム単位毎にアクセス位置を指定する2つの拡張URI情報を前記パケット受信装置に提示するアクセス位置通知手段を備える

ことを特徴とする請求項25記載のパケット送信装置。

[27] 前記2つの拡張URI情報は、Universal Plug and Play(UPnP)におけるresのURI指定に使用し、前記2つのMIME-Typeは前記resのattributeであるproto

colInfoの第3フィールドに挿入することによりコンテンツの識別を行う

ことを特徴とする請求項26記載のパケット送信装置。

[28] 前記伝送手段は、HTTPによる伝送とRTPによる伝送を切り替えて前記AVデータを伝送する

ことを特徴とする請求項1記載のパケット送信装置。

[29] 前記伝送手段は、前記HTTPによる伝送として、前記パケット送信装置の出力がライブ放送の受信信号またはライブ放送の受信チャネルの切り替えまたは蓄積されたプログラム選択時の再生信号の場合には、チャンク伝送を行い、プログラム選択後の蓄積メディアから再生されたプログラムからの再生信号の場合には、レンジリクエストを用いて再生を切替えて行う

ことを特徴とする請求項28記載のパケット送信装置。

[30] 前記伝送手段は、SMPTE259M規格で規定された非圧縮SD方式信号、SMPTE292M規格で規定された非圧縮HD形式、IEC61883規格で規定されたIEEE1394によるDVまたはデジタル放送のMPEG－TSの伝送ストリーム形式、DVB規格A010で規定されたDVB－ASIによるMPEG－TS形式、MPEG－PES，MPEG－ES、MPEG4、ISO／IEC H．264の内のいずれか一つのデータストリーム形式で、前記AVデータを伝送する

ことを特徴とする請求項1記載のパケット送信装置。

[31] 前記パケット化手段は、前記AVデータを構成するデータブロックにタイムスタンプを付加し、1つ以上のタイムスタンプ付データブロックをまとめてRTPまたはHTTPのペイロードとしてマッピングすることによって前記パケット化を行う

ことを特徴とする請求項30記載のパケット送信装置。

[32] 前記パケット化手段は、前記AVデータをMPEG－TSで伝送する場合、各TSパケットにタイムスタンプを付加し、複数のタイムスタンプ付TSパケットをまとめてRTPまたはHTTP上にマッピングする

ことを特徴とする請求項31記載のパケット送信装置。

[33] 前記各TSパケットに付加するタイムスタンプのクロックはMPEGのシステムクロック周波数に等しく、

前記パケット送信装置はさらに、前記TSパケットを受信し、受信したTSパケットに付加されたタイムスタンプより、MPEG－TSのネットワーク伝送によりProgram Clock Reference（PCR）に付加された伝送ジッターを除去して、MPEGシステムクロックの再生を行うクロック再生手段を備える

ことを特徴とする請求項32記載のパケット送信装置。

[34] 前記パケット化手段は、外部入力されたTSに付加されたタイムスタンプの有効ビット数または蓄積メディアから再生されたTSに付加されたタイムスタンプの有効ビット数が前記各TSパケットに付加するタイムスタンプの有効ビット数と異なる場合において、ストリームのMPEGのPCRが不連続になりシステムタイムベースの不連続が発生しないとき、また、TSのcontinuity__counterの不連続が発生しないときは、前記外部入力されたTSに付加されたタイムスタンプまたは前記蓄積メディアから再生されたTSに付加されたタイムスタンプと、前記TSパケットに付加するタイムスタンプとを変えずに載せ変えだけを行ない、ストリームのMPEGのPCRが不連続になりシステムタイムベースの不連続が発生するポイントまたはTSのcontinuity__counterの不連続が発生するときは、前記不連続の発生点でTSの不連続発生を通知するTSパケットを挿入することで、前記パケット化を行う

ことを特徴とする請求項32記載のパケット送信装置。

[35] 前記伝送手段は、Nを1以上の整数とした場合、UDPまたはTCPのN個のポートを用いて、前記AVデータにより構成されるN個のプログラムを前記N個のポートのそれぞれに割り当てて伝送する

ことを特徴とする請求項1記載のパケット送信装置。

[36] 前記N個のポートのそれぞれに割り当てるN個のプログラムは、それぞれ、前記パケット送信装置に内蔵された放送受信チューナまたは蓄積メディアデバイスがUPnP手段のコンテナ形式で表現され、放送受信チャネルまたは蓄積プログラムがUPnP手段のitem形式で表現され、それぞれのitemの存在位置がURIでUPnP手段の＜res protocolInfo＞形式にマッピングされている

ことを特徴とする請求項35記載のパケット送信装置。

[37] 前記N個のポートのそれぞれに割り当てるN個のプログラムは、前記パケット送信装

置から前記パケット受信装置への伝送ストリームが存在する場合に、UPnPのproperty形式で表われ、

前記伝送ストリームのpropertyのattributeが前記チューナのコンテナの種別、前記チューナのコンテナ種別ごとのチューナID、前記チューナで選局されたチャネルID、前記伝送ストリームの共有を含む利用可否情報、前記ストリームを伝送するトランスポート層が使用するTCPまたはRTPのポート番号、前記パケット受信装置におけるUPnP—AV手段のConnectionManagerが前記パケット送信装置におけるConnectionManagerに対して前記itemに関する論理的接続に関連して設定するUPnP—AV手段のconnectionID、および、前記パケット送信装置におけるUPnP—AV手段のConnectionManagerが前記パケット受信装置におけるConnectionManagerに対して前記itemに関する論理的接続に関連して設定するUPnP—AVのconnectionIDの少なくとも1つを含んでおり、

前記パケット送信装置はさらに、前記パケット受信装置として前記パケット送信装置内のチューナのチャネル選局を行なう時に、前記伝送ストリームのpropertyを参照することにより、伝送ストリームに空きあるか無いか、およびどのチューナの、どのチャネルが選局されているかを判別する受信制御手段を備える

ことを特徴とする請求項36記載のパケット送信装置。

[38] 前記N個のポートのそれぞれに割り当てるN個のプログラムは、前記パケット送信装置から前記パケット受信装置への伝送ストリームが存在する場合に、UPnPのproperty形式で表わされ、

前記伝送ストリームのpropertyのattributeが前記蓄積メディアデバイスのコンテナの種別、前記蓄積メディアデバイスのコンテナ種別ごとの蓄積メディアデバイスID、前記蓄積メディアデバイスで選択されたプログラムID、前記伝送ストリームの共有を含む利用可否情報、前記ストリームを伝送するトランスポート層が使用するTCPまたはRTPのポート番号、前記パケット受信装置におけるUPnP—AV手段のConnectionManagerが前記パケット送信装置におけるConnectionManagerに対して前記itemに関する論理的接続に関連して設定するUPnP—AV手段のconnectionID、および、前記パケット送信装置におけるUPnP—AV手段のConnectionManager

が前記パケット受信装置におけるConnectionManagerに対して前記itemに関する論理的接続に関連して設定するUPnP－AV手段のconnectionIDの少なくとも1つを含んでおり、

前記パケット送信装置はさらに、前記パケット受信装置として前記パケット送信装置内の蓄積メディアデバイスのプログラム選択を行なう時に、前記伝送ストリームのpropertyを参照することにより、伝送ストリームに空きあるか無いか、およびどの蓄積メディアデバイスのどのプログラムが選択されているかを判別する受信制御手段を備える

ことを特徴とする請求項36記載のパケット送信装置。

[39] 「前記ストリームを伝送するトランスポート層が使用するTCPまたはUDPのポート番号」、および、「前記パケット受信装置におけるUPnP－AV手段のConnectionManagerが前記パケット送信装置におけるConnectionManagerに対して前記itemに関する論理的接続に関連して設定するUPnP－AV手段のconnectionID、または前記パケット送信装置におけるUPnP－AV手段のConnectionManagerが前記パケット受信装置におけるConnectionManagerに対して前記itemに関する論理的接続に関連して設定するUPnP－AV手段のconnectionID」の論理対により、前記UPnP－AV手段と、前記TCPまたは前記UDPを使用するHTTPまたはRTPを用いるトランスポート手段とが論理的に対応づけられる

ことを特徴とする請求項1または37または38記載のパケット送信装置。

[40] パケット受信装置にパケットデータを送信するパケット送信方法であって、

AVデータが入力される端子を示す入力端子情報、前記AVデータのデータフォーマットを示すデータフォーマット情報及び前記AVデータの属性を示す属性情報を含むAVデータ情報を取得するAVデータ情報取得ステップと、

前記AVデータ及び非AVデータの入力を受け付けるデータ入力ステップと、

前記非AVデータまたは前記AVデータより、前記AVデータの課金情報、再生制御情報及びコピー制御情報の少なくとも1つの情報を抽出し、抽出した情報から、前記AVデータを送信する際の条件となる暗号化モードを示す暗号化モード情報を生成する送信条件設定管理ステップと、

前記入力端子情報、前記データフォーマット情報及び前記属性情報を組み合わせ

て決定される送信条件に基づいて、前記データ入力ステップで入力された前記AVデータを暗号化し、暗号化された前記AVデータに対して前記暗号化モード情報に基づく暗号化情報ヘッダを付加することによって暗号化データを生成する暗号化データ生成ステップと、

前記暗号化データ生成ステップで生成された暗号化データに対して、パケットヘッダを付加することによってパケットを生成するパケット化ステップと、

前記パケット受信装置との間で認証処理を行う認証ステップと、

前記入力端子情報、前記属性情報及び前記パケット受信装置より指定される送信モードを示す情報の少なくとも1つを用いて、前記パケット送信装置と前記パケット受信装置の間での前記AVデータの伝送プロトコルを決定する伝送プロトコル決定ステップと、

前記認証処理によって前記パケット受信装置との認証処理が完了した後に、前記伝送プロトコル決定ステップで決定された伝送プロトコルに従って、前記パケット化ステップによって生成された暗号化データを含むパケットを前記パケット受信装置に伝送する伝送ステップと

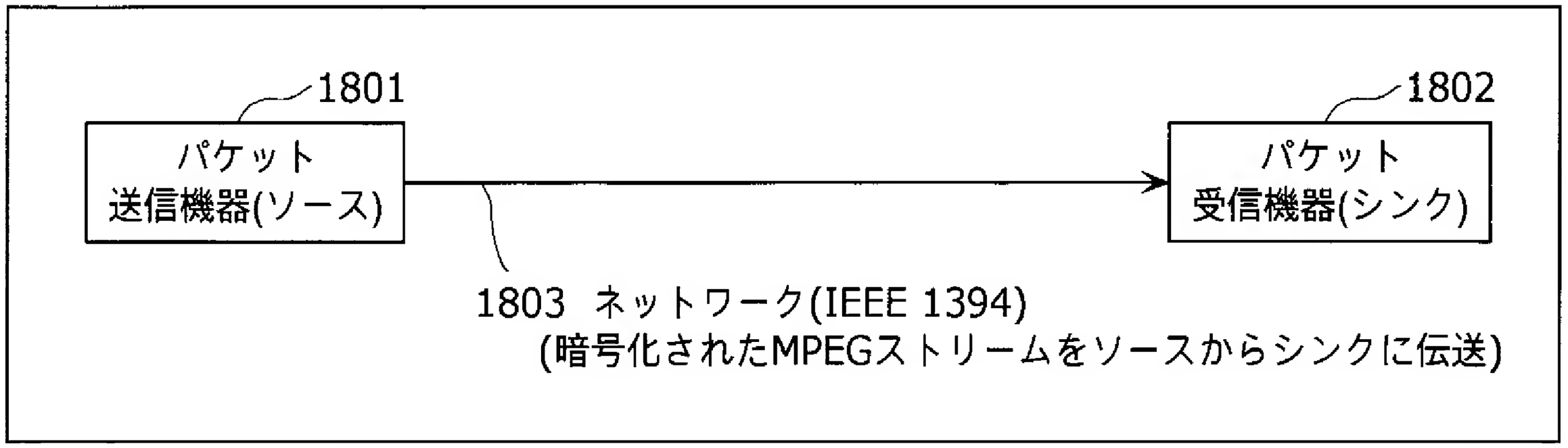
を含むことを特徴とするパケット送信方法。

[41] パケット受信装置にパケットデータを送信するパケット送信装置のためのプログラムであって、

請求項40記載のパケット送信方法に含まれるステップをコンピュータに実行させることを特徴とするプログラム。

[図1]

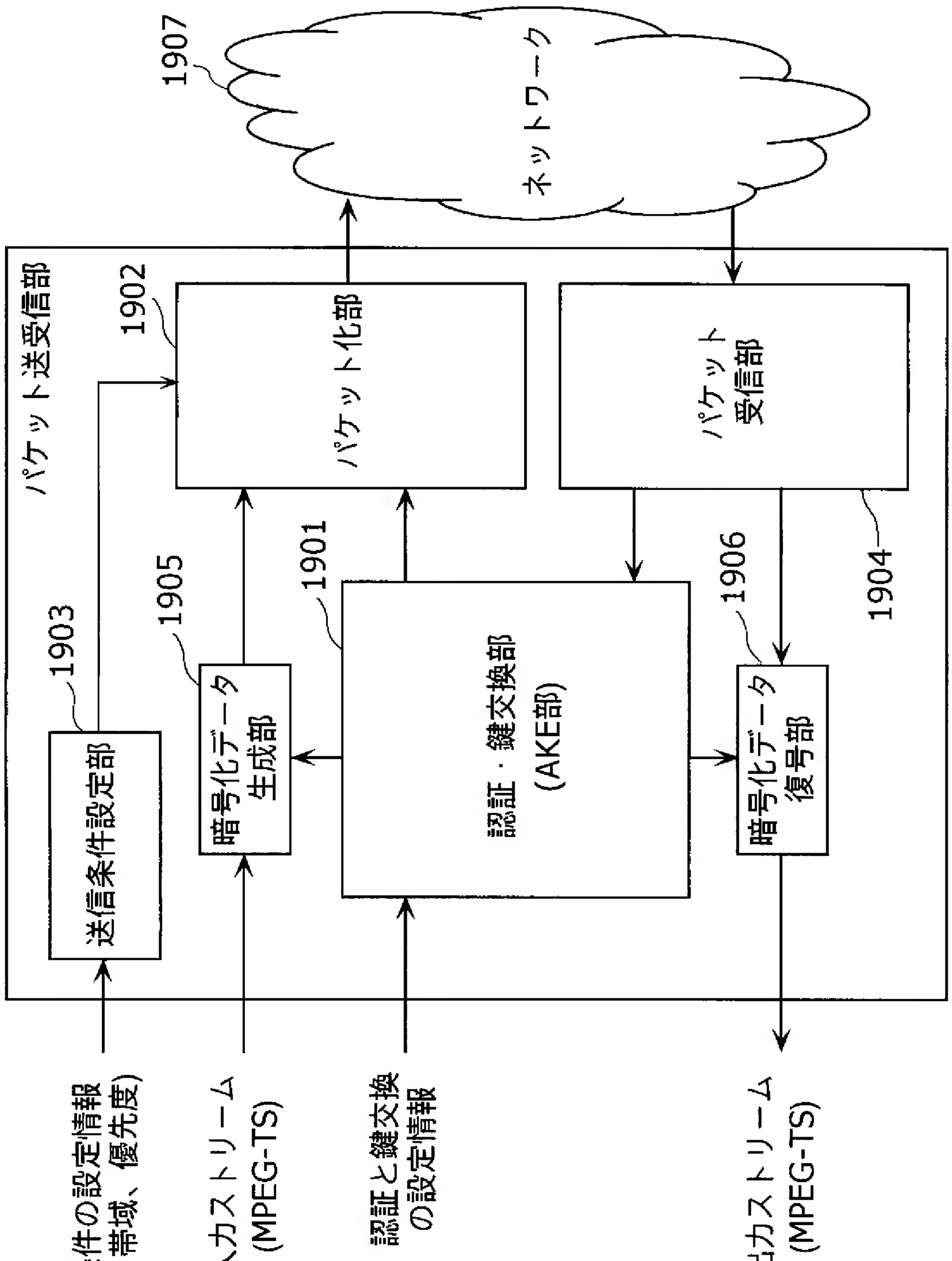
(a)



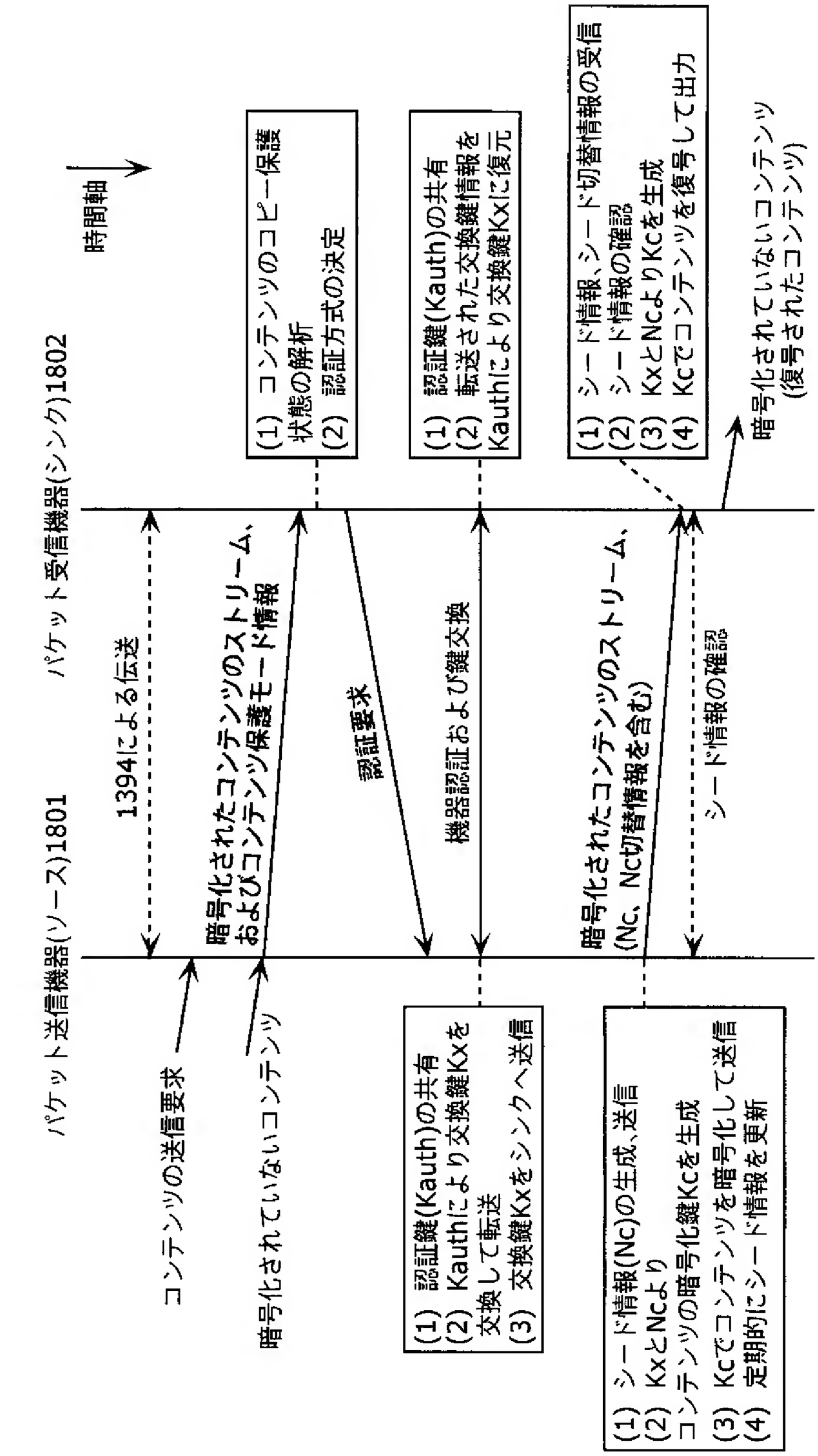
(b)

送信機器(ソース)の例	受信機器(シンク)の例	コンテンツ伝送における暗号化
DVHS	DVHS	MPEG-TSにDTCP方式によるコンテンツ保護を実施
HDDレコーダ	HDDレコーダ	
1394搭載STB	1394搭載STB	
1394搭載ディジタルTV	1394搭載ディジタルTV	

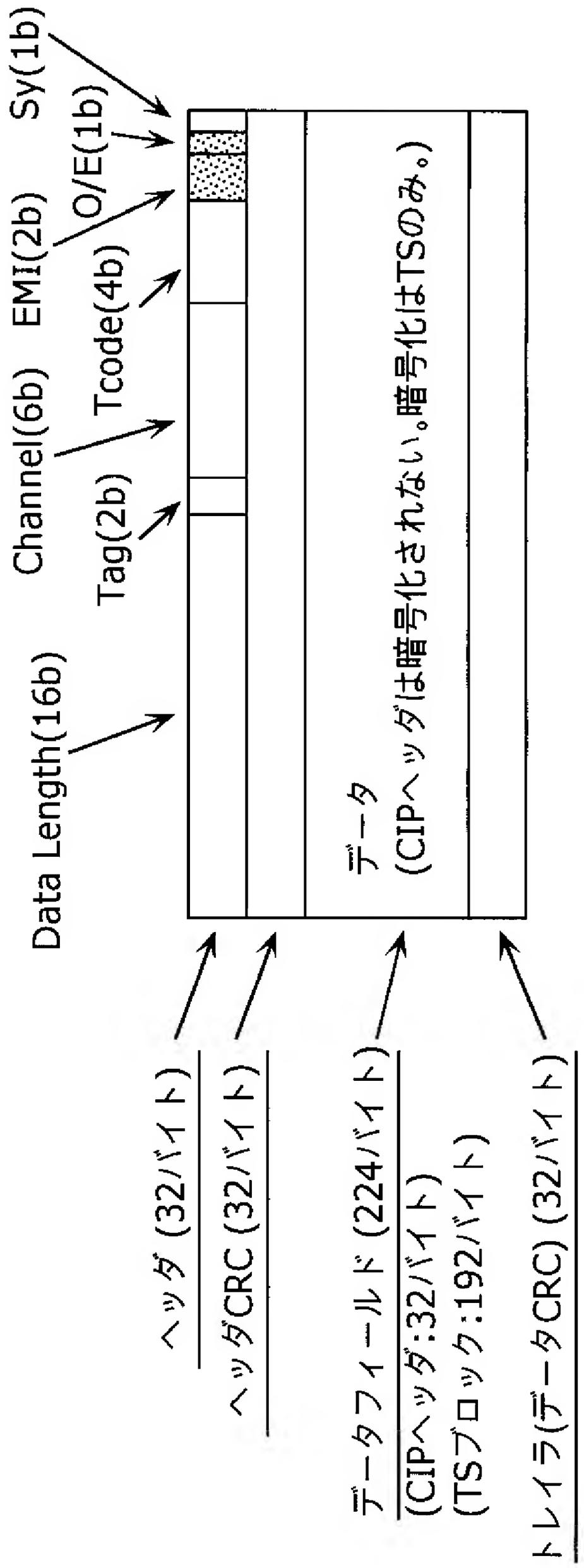
[図2]


1907
ネットワーク
パケット送受信部
1902
パケット化部
パケット
受信部
1904
1903
送信条件設定部
1905
暗号化データ
生成部
1901
認証・鍵交換部
(AKE部)
1906
暗号化データ
復号部
送信条件の設定情報
(バス、帯域、優先度)
入力ストリーム
(MPEG-TS)
認証と鍵交換
の設定情報
出力ストリーム
(MPEG-TS)

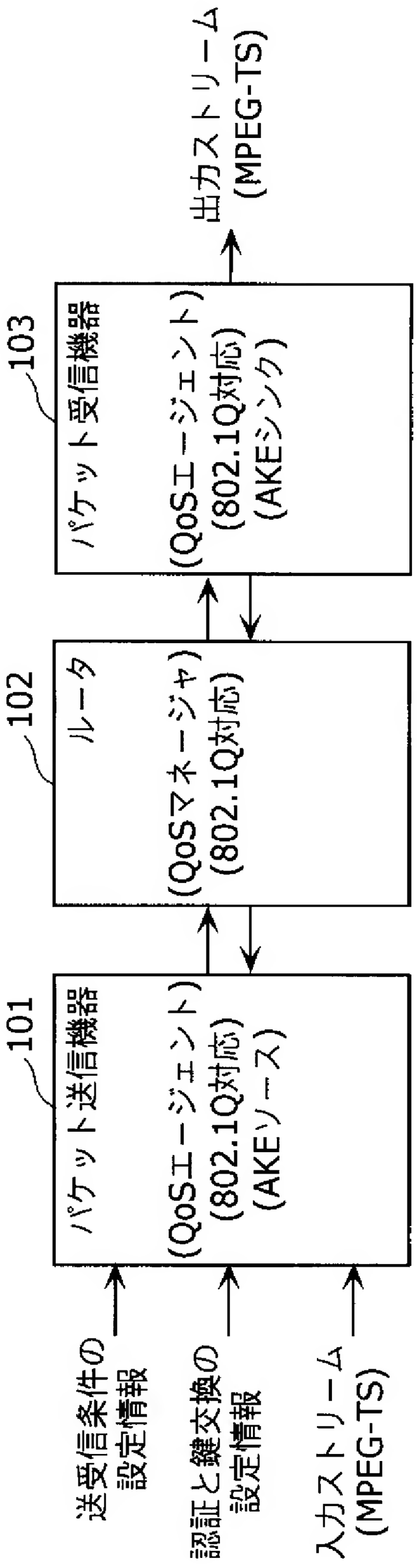
[図3]


時間軸
パケット送信機器(ソース)1801
パケット受信機器(シンク)1802
1394による伝送
暗号化されたコンテンツのストリーム、
およびコンテンツ保護モード情報
認証要求
機器認証および鍵交換
暗号化されたコンテンツのストリーム、
(Nc、Nc切替情報を含む)
シード情報の確認
コンテンツの送信要求
暗号化されていないコンテンツ
(1) コンテンツのコピー保護
状態の解析
(2) 認証方式の決定
(1) 認証鍵(Kauth)の共有
(2) 転送された交換鍵情報を
Kauthにより交換鍵Kxに復元
(1) シード情報、シード切替情報の受信
(2) シード情報の確認
(3) KxとNcよりKcを生成
(4) Kcでコンテンツを復号して出力
暗号化されていないコンテンツ
(復号されたコンテンツ)
(1) 認証鍵(Kauth)の共有
(2) Kauthにより交換鍵Kxを
交換して転送
(3) 交換鍵Kxをシンクへ送信
(1) シード情報(Nc)の生成、送信
(2) KxとNcより
コンテンツの暗号化鍵Kcを生成
(3) Kcでコンテンツを暗号化して送信
(4) 定期的にシード情報を更新

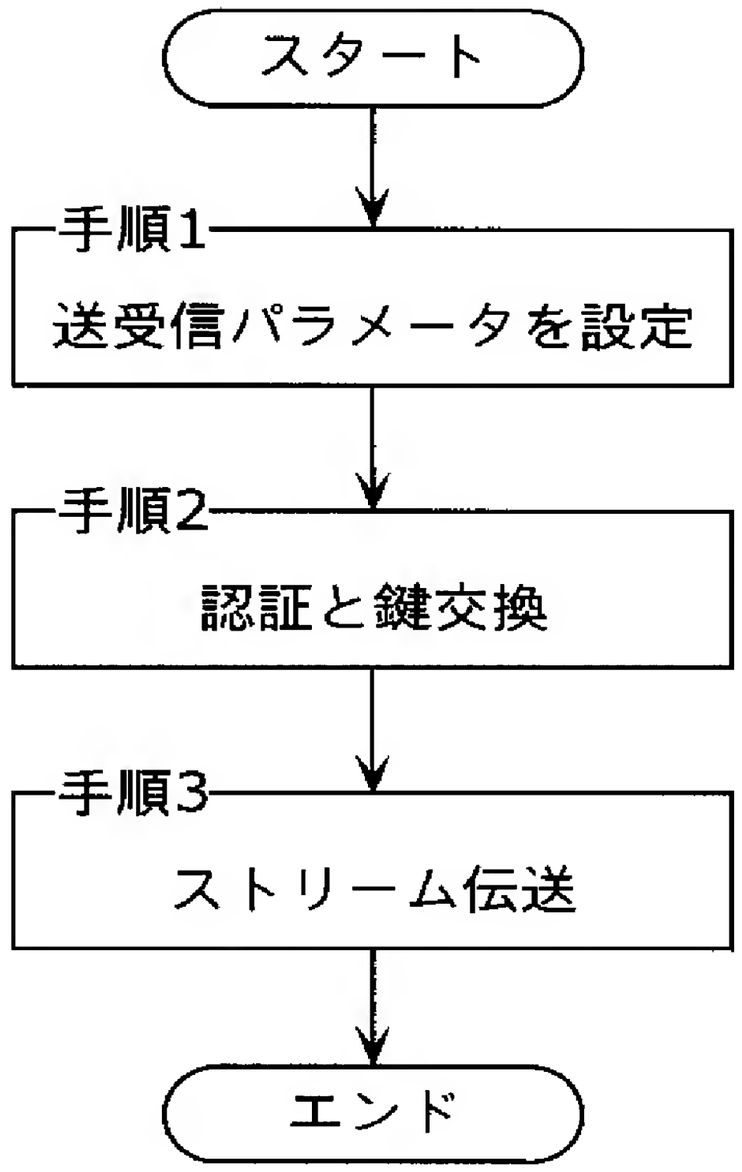
[図4]


Sy(1b)
O/E(1b)
EMI(2b)
Tcode(4b)
Channel(6b)
Tag(2b)
Data Length(16b)
データ
(CIPヘッダは暗号化されない。暗号化はTSのみ。)
ヘッダ (32バイト)
ヘッダCRC (32バイト)
データフィールド (224バイト)
(CIPヘッダ:32バイト)
(TSブロック:192バイト)
トレイラ(データCRC) (32バイト)

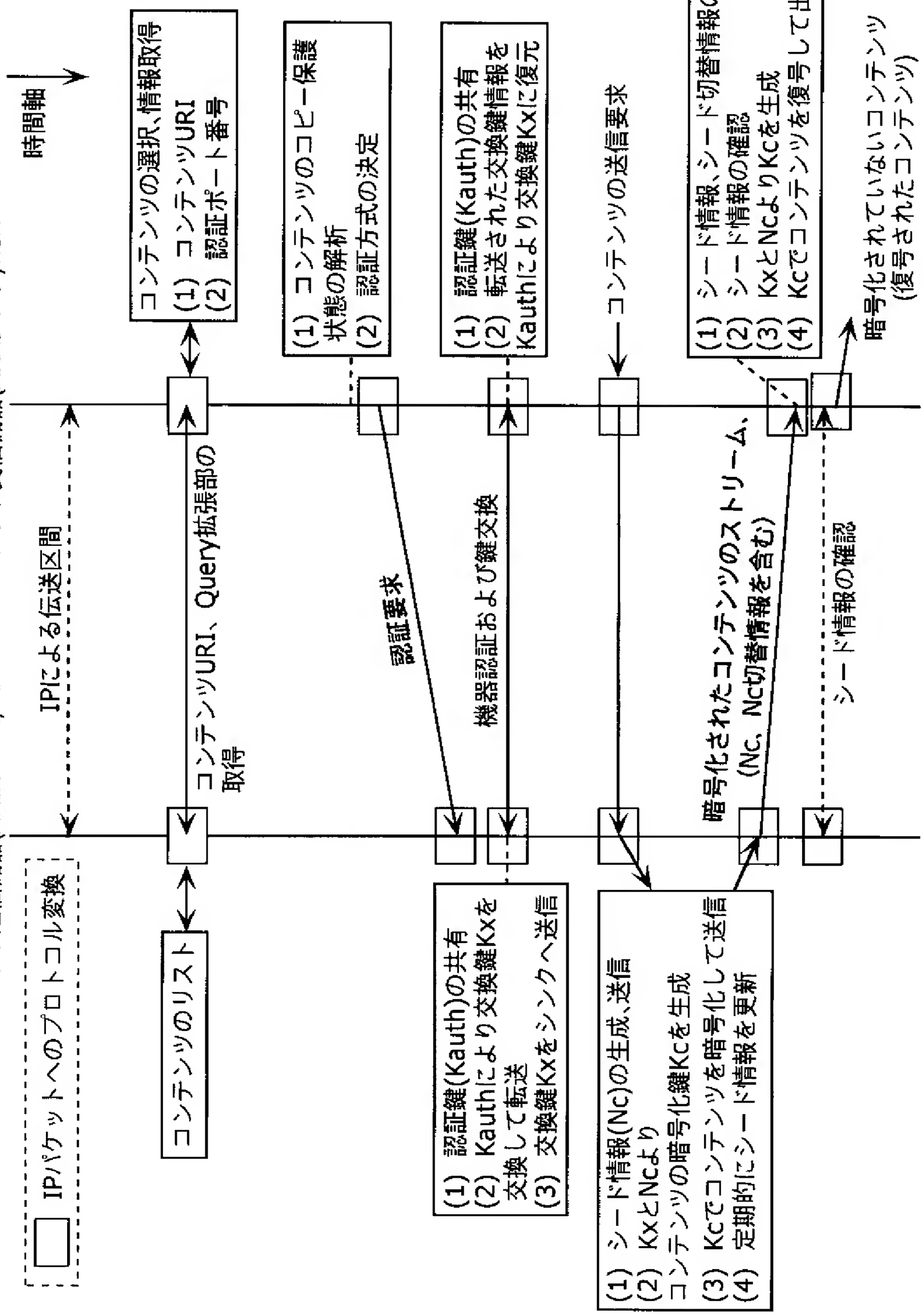
[図5]


103
パケット受信機器
(QoSエージェント)
(802.1Q対応)
(AKEシンク)
出力ストリーム
(MPEG-TS)
102
ルータ
(QoSマネージャ)
(802.1Q対応)
101
パケット送信機器
(QoSエージェント)
(802.1Q対応)
(AKEソース)
送受信条件の
設定情報
認証と鍵交換の
設定情報
入力ストリーム
(MPEG-TS)

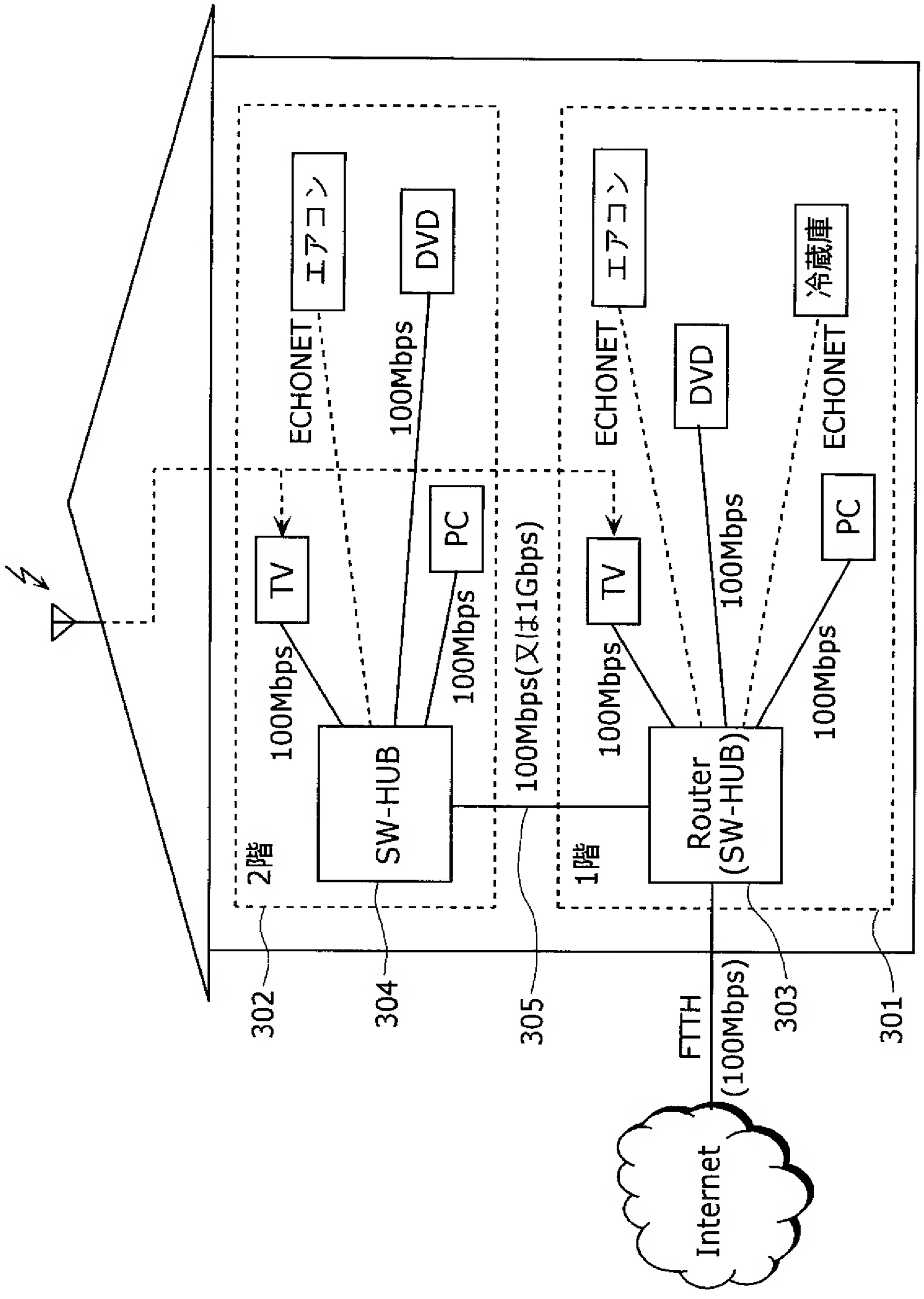
[図6]



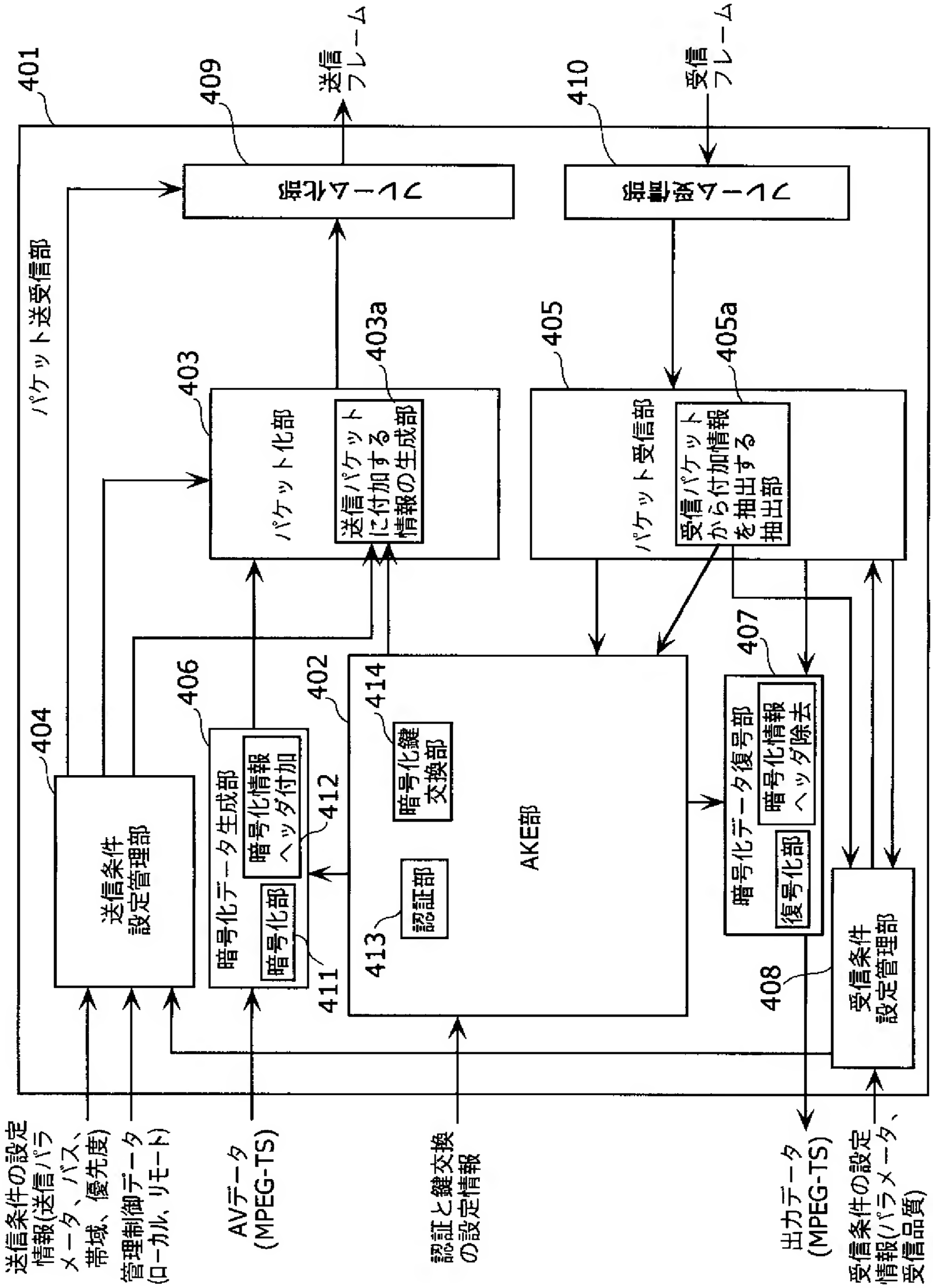
[図7]


時間軸
パケット送信機器(AKEソース)101
パケット受信機器(AKEシンク)102
IPによる伝送区間
IPパケットへのプロトコル変換
コンテンツのリスト
コンテンツの選択、情報取得
(1) コンテンツURI
(2) 認証ポート番号
コンテンツURI、Query拡張部の取得
(1) コンテンツのコピー保護状態の解析
(2) 認証方式の決定
認証要求
(1) 認証鍵(Kauth)の共有
(2) Kauthにより交換鍵Kxを交換して転送
(3) 交換鍵Kxをシンクへ送信
機器認証および鍵交換
(1) 認証鍵(Kauth)の共有
(2) 転送された交換鍵情報をKauthにより交換鍵Kxに復元
コンテンツの送信要求
(1) シード情報(Nc)の生成、送信
(2) KxとNcより
コンテンツの暗号化鍵Kcを生成
(3) Kcでコンテンツを暗号化して送信
(4) 定期的にシード情報を更新
暗号化されたコンテンツのストリーム、
(Nc、Nc切替情報を含む)
(1) シード情報、シード切替情報の受信
(2) シード情報の確認
(3) KxとNcよりKcを生成
(4) Kcでコンテンツを復号して出力
暗号化されていないコンテンツ
(復号されたコンテンツ)
シード情報の確認

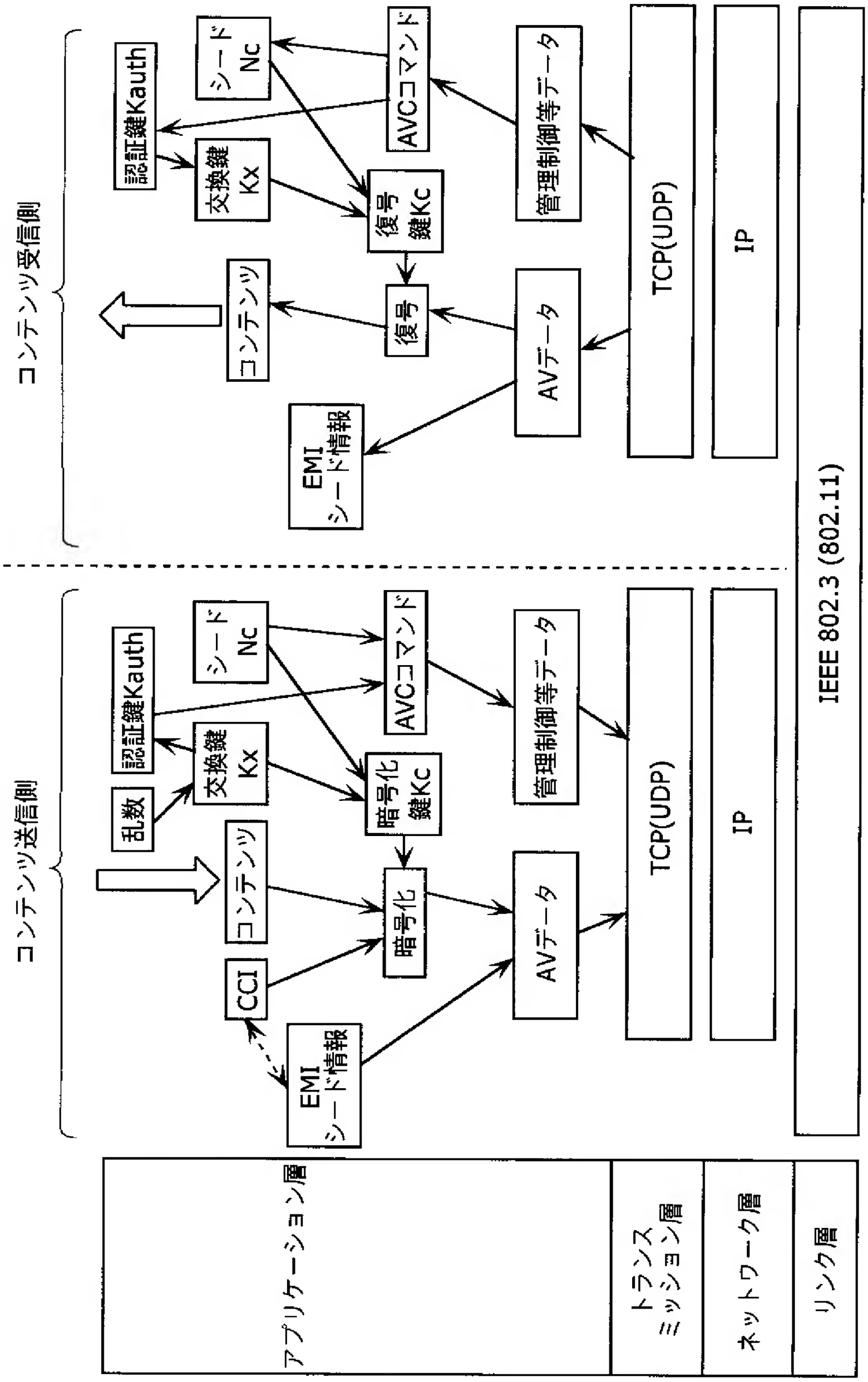
[図8]


エアコン
DVD
ECHONET
100Mbps
TV
PC
100Mbps
SW-HUB
100Mbps(又は1Gbps)
2階
エアコン
冷蔵庫
ECHONET
DVD
100Mbps
TV
PC
100Mbps
Router
(SW-HUB)
1階
302
304
305
FTTH
(100Mbps)
303
301
Internet

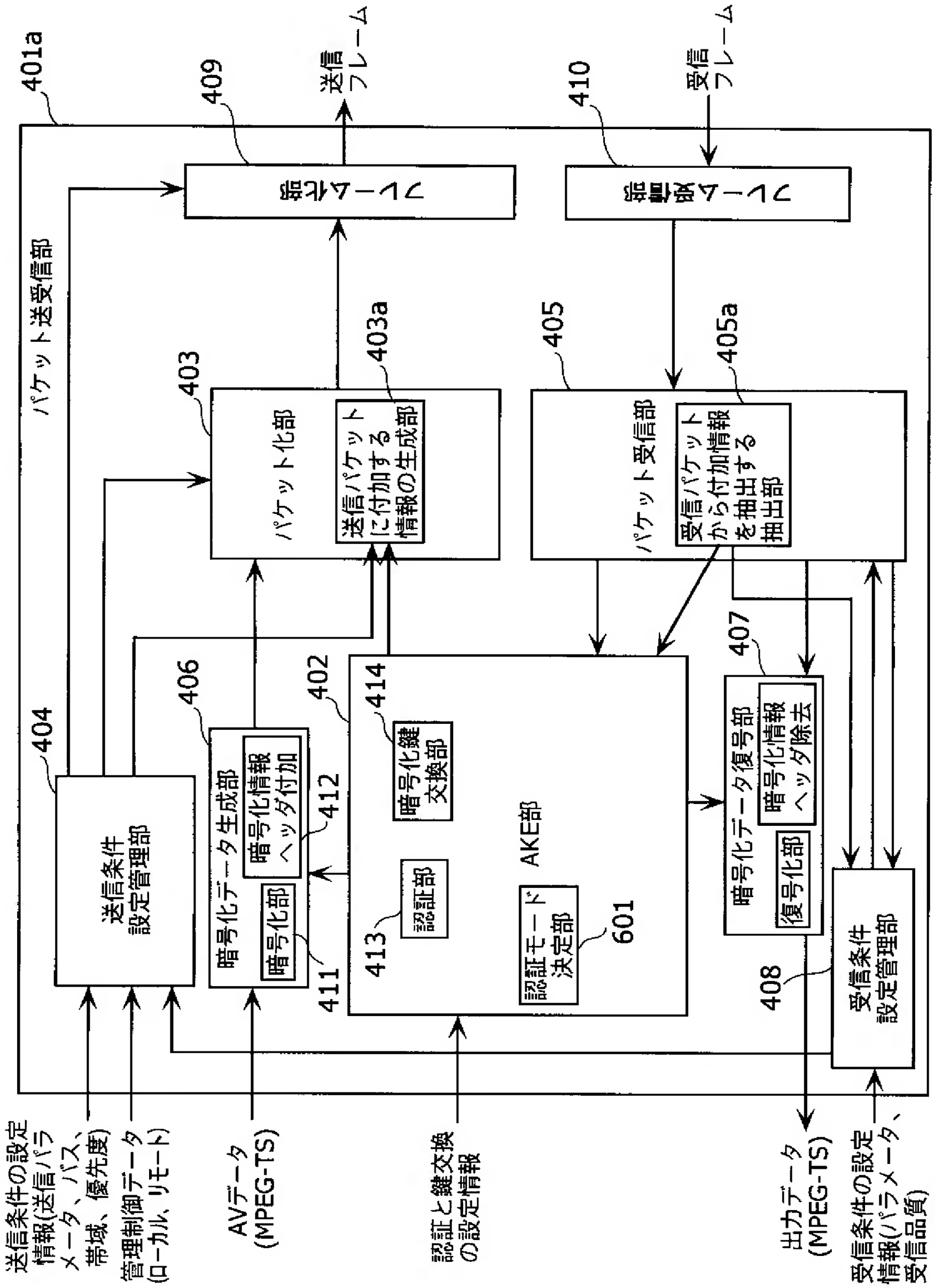
[図9]


401
409
送信フレーム
410
受信フレーム
フレーム化部
フレーム受信部
パケット送受信部
403
パケット化部
403a
送信パケットに付加する情報の生成部
405
パケット受信部
405a
受信パケットから付加情報を抽出する抽出部
404
送信条件設定管理部
406
暗号化データ生成部
暗号化情報ヘッダ付加
412
暗号化部
411
402
AKE部
414
暗号化鍵交換部
413
認証部
407
暗号化データ復号部
暗号化情報ヘッダ除去
復号化部
408
受信条件設定管理部
送信条件の設定情報(送信パラメータ、バス、帯域、優先度)
管理制御データ(ローカル、リモート)
AVデータ(MPEG-TS)
認証と鍵交換の設定情報
出力データ(MPEG-TS)
受信条件の設定情報(パラメータ、受信品質)

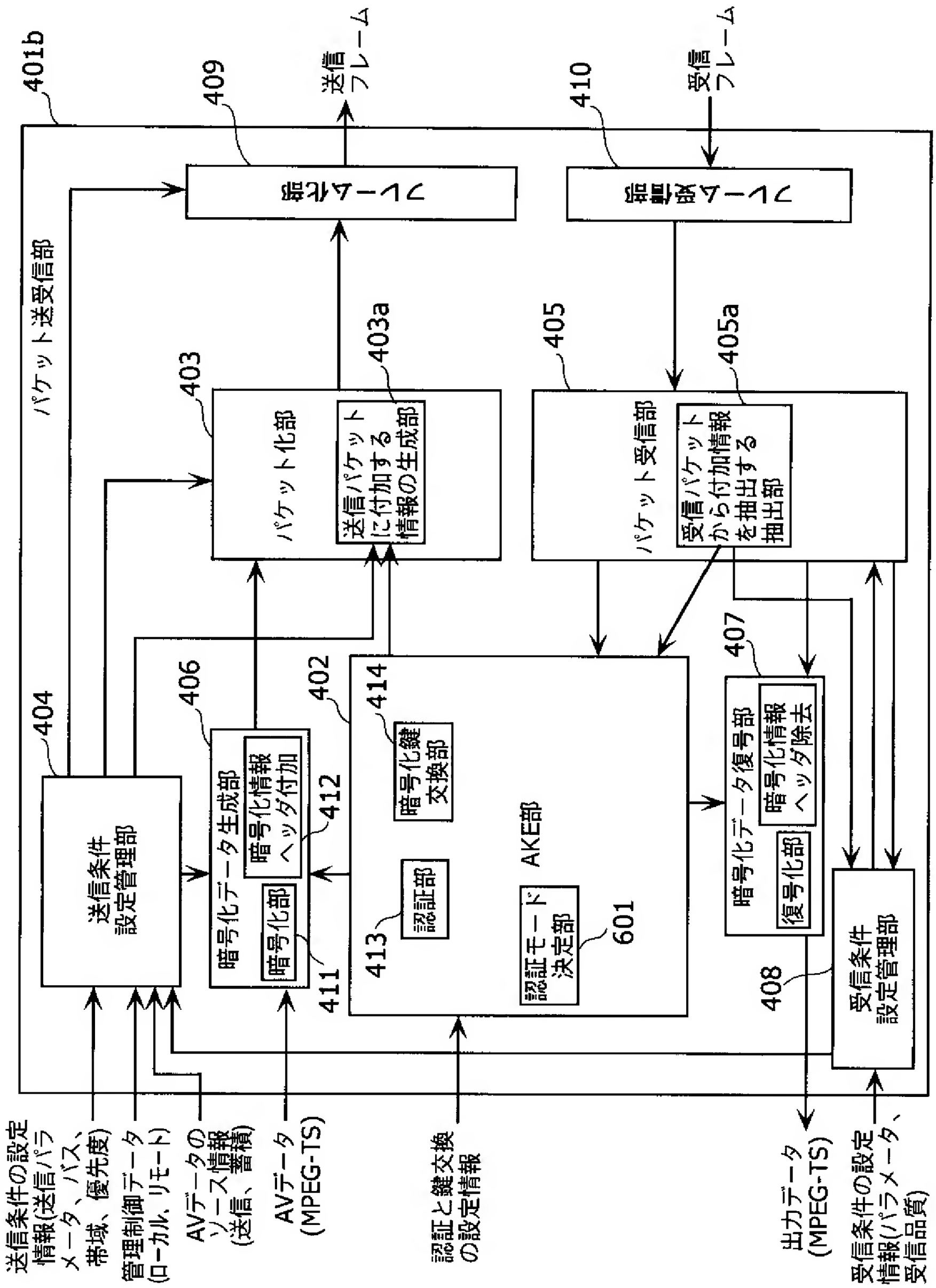
[図10]


コンテンツ受信側
認証鍵Kauth
シード Nc
交換鍵 Kx
AVCコマンド
復号 鍵Kc
管理制御等データ
コンテンツ
復号
AVデータ
TCP(UDP)
IP
EMI シード情報
コンテンツ送信側
乱数
認証鍵Kauth
シード Nc
交換鍵 Kx
AVCコマンド
暗号化 鍵Kc
管理制御等データ
コンテンツ
CCI
暗号化
AVデータ
TCP(UDP)
IP
EMI シード情報
IEEE 802.3 (802.11)
アプリケーション層
トランス ミッション層
ネットワーク層
リンク層

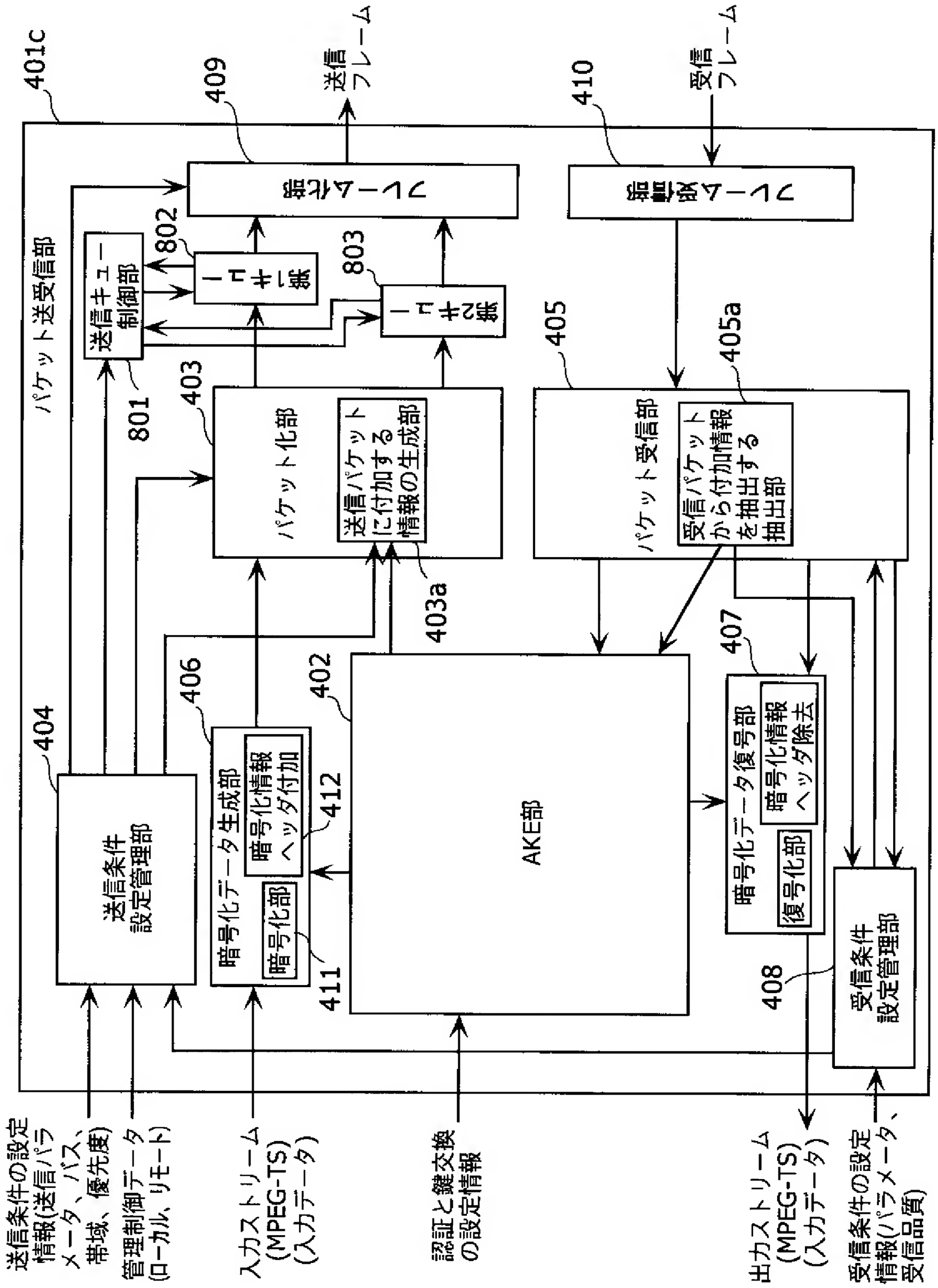
[図11]


401a
409
送信フレーム
410
受信フレーム
フレーム化部
フレーム受信部
パケット送受信部
403a
405a
405
403
パケット化部
送信パケットに付加する情報の生成部
パケット受信部
受信パケットから付加情報を抽出する抽出部
404
406
402
414
407
送信条件設定管理部
暗号化データ生成部
暗号化情報ヘッダ付加
412
暗号化鍵交換部
暗号化データ復号部
暗号化情報ヘッダ除去
暗号化部
411
413
認証部
AKE部
認証モード決定部
601
復号化部
408
受信条件設定管理部
送信条件の設定情報(送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル、リモート)
AVデータ(MPEG-TS)
認証と鍵交換の設定情報
出力データ(MPEG-TS)
受信条件の設定情報(パラメータ、受信品質)

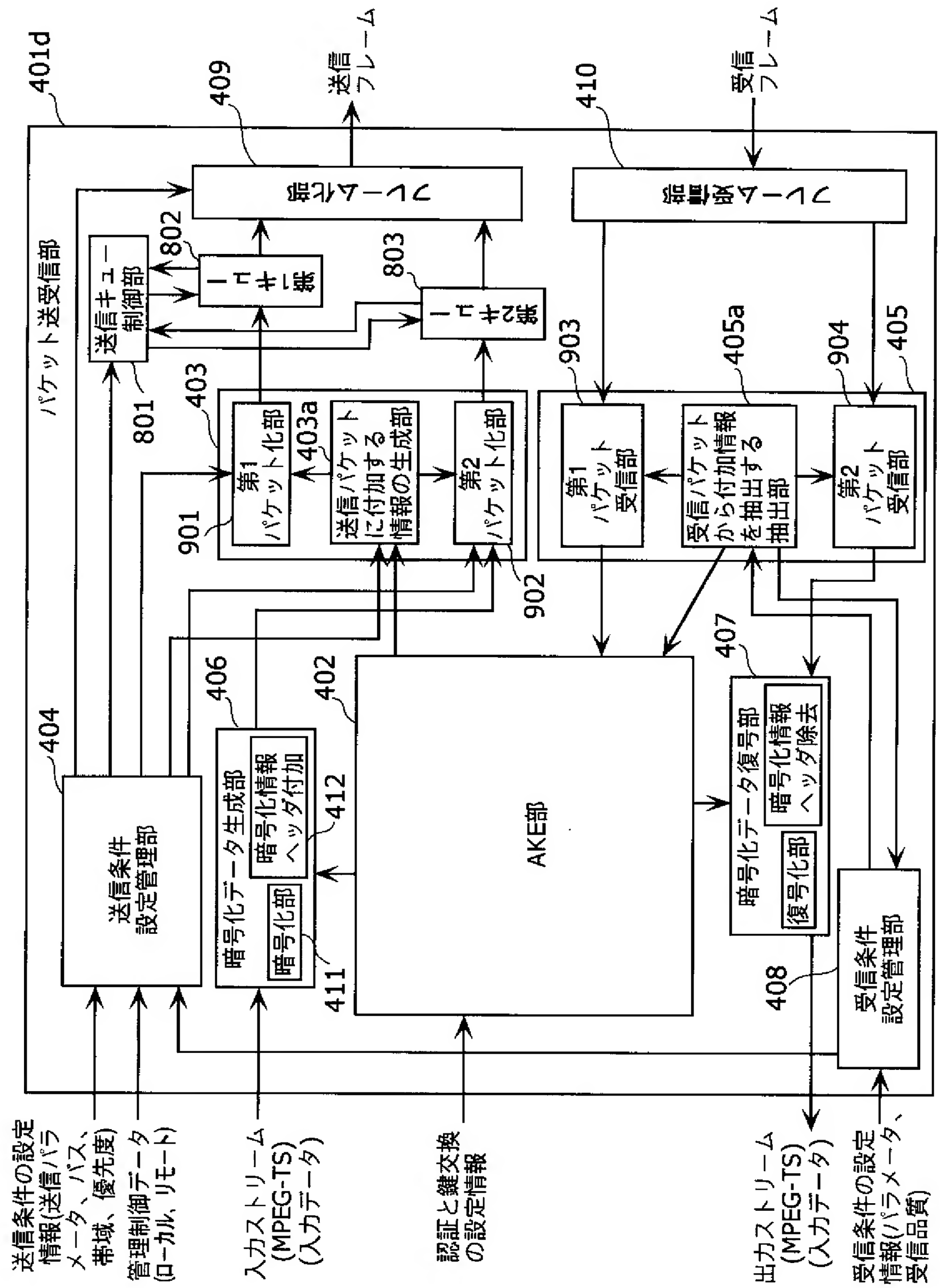
[図12]


401b
409
送信フレーム
410
受信フレーム
フレーム化部
フレーム受信部
パケット送受信部
403
パケット化部
送信パケットに付加する情報の生成部
403a
405
パケット受信部
受信パケットから付加情報を抽出する抽出部
405a
404
送信条件設定管理部
406
暗号化データ生成部
暗号化情報ヘッダ付加
412
暗号化部
411
402
414
暗号化鍵交換部
413
認証部
AKE部
認証モード決定部
601
407
暗号化データ復号部
暗号化情報ヘッダ除去
復号化部
408
受信条件設定管理部
送信条件の設定情報(送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル、リモート)
AVデータのソース情報(送信、蓄積)
AVデータ(MPEG-TS)
認証と鍵交換の設定情報
出力データ(MPEG-TS)
受信条件の設定情報(パラメータ、受信品質)

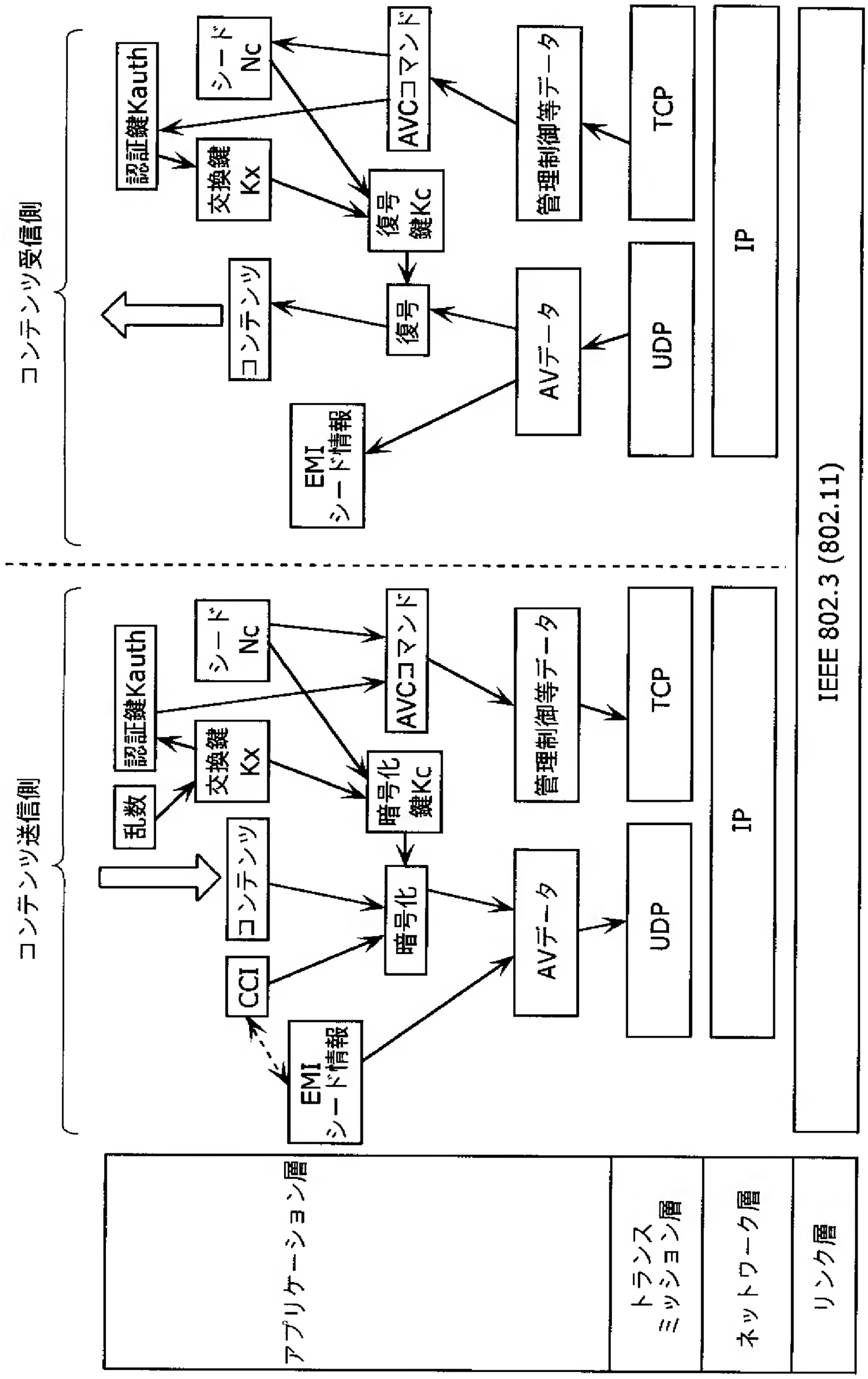
[図13]


401c
409
送信フレーム
410
受信フレーム
プレーム化部
プレーム受信部
802
803
送信キュー制御部
第1キュー
第2キュー
405
405a
403
801
パケット化部
送信パケットに付加する情報の生成部
パケット受信部
受信パケットから付加情報を抽出する抽出部
403a
407
406
402
404
暗号化データ生成部
暗号化情報ヘッダ付加
412
AKE部
暗号化データ復号部
暗号化情報ヘッダ除去
復号化部
暗号化部
411
408
送信条件設定管理部
受信条件設定管理部
送信条件の設定情報(送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル、リモート)
入力ストリーム(MPEG-TS)(入力データ)
認証と鍵交換の設定情報
出力ストリーム(MPEG-TS)(入力データ)
受信条件の設定情報(パラメータ、受信品質)

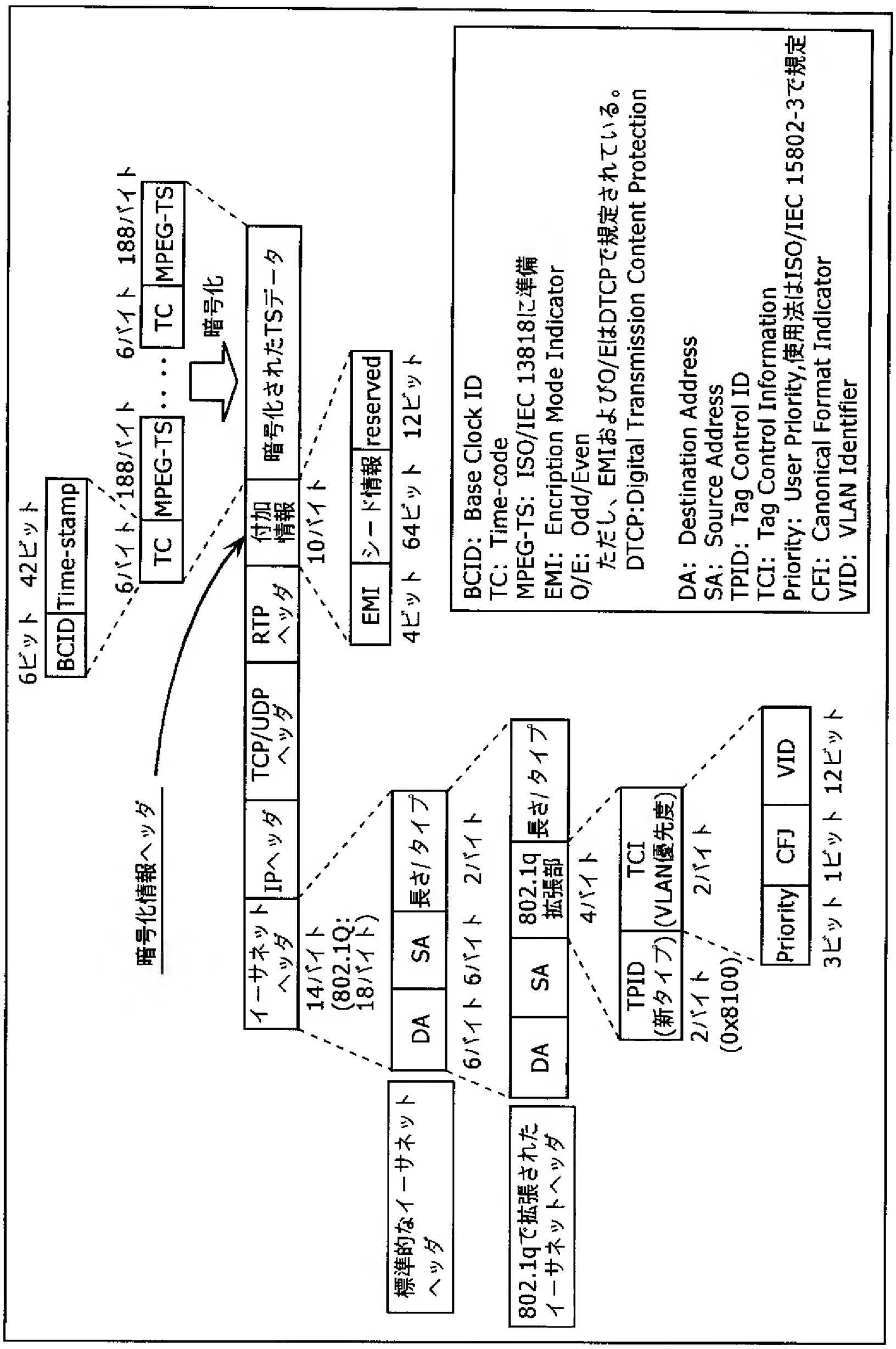
[図14]


401d
409
送信フレーム
410
受信フレーム
フレーム化部
フレーム受信部
802
803
送信キュー制御部
第1キュー
第2キュー
903
405a
904
405
801
403
第1パケット化部
403a
送信パケットに付加する情報の生成部
第2パケット化部
第1パケット受信部
受信パケットから付加情報を抽出する抽出部
第2パケット受信部
901
902
407
406
402
404
暗号化データ生成部
暗号化情報ヘッダ付加
暗号化部
AKE部
暗号化データ復号部
暗号化情報ヘッダ除去
復号化部
412
411
408
送信条件設定管理部
受信条件設定管理部
送信条件の設定情報(送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル, リモート)
入力ストリーム(MPEG-TS)(入力データ)
認証と鍵交換の設定情報
出力ストリーム(MPEG-TS)(入力データ)
受信条件の設定情報(パラメータ、受信品質)

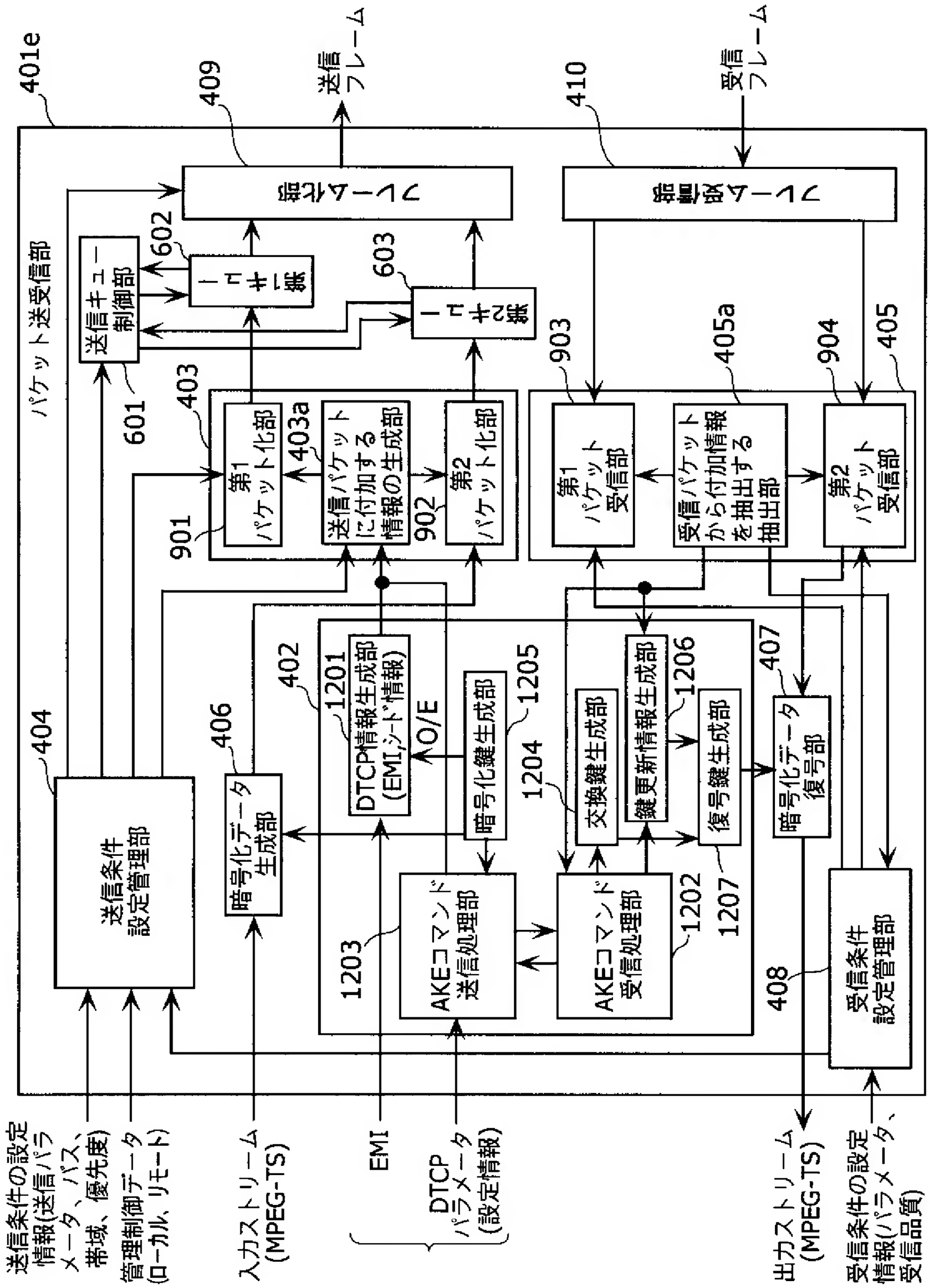
[図15]


コンテンツ受信側
認証鍵Kauth
シード Nc
AVCコマンド
交換鍵 Kx
復号 鍵Kc
管理制御等データ
TCP
IP
コンテンツ
復号
AVデータ
UDP
EMI シード情報
コンテンツ送信側
乱数
暗号化 鍵Kc
暗号化
CCI
アプリケーション層
トランス ミッション層
ネットワーク層
リンク層
IEEE 802.3 (802.11)

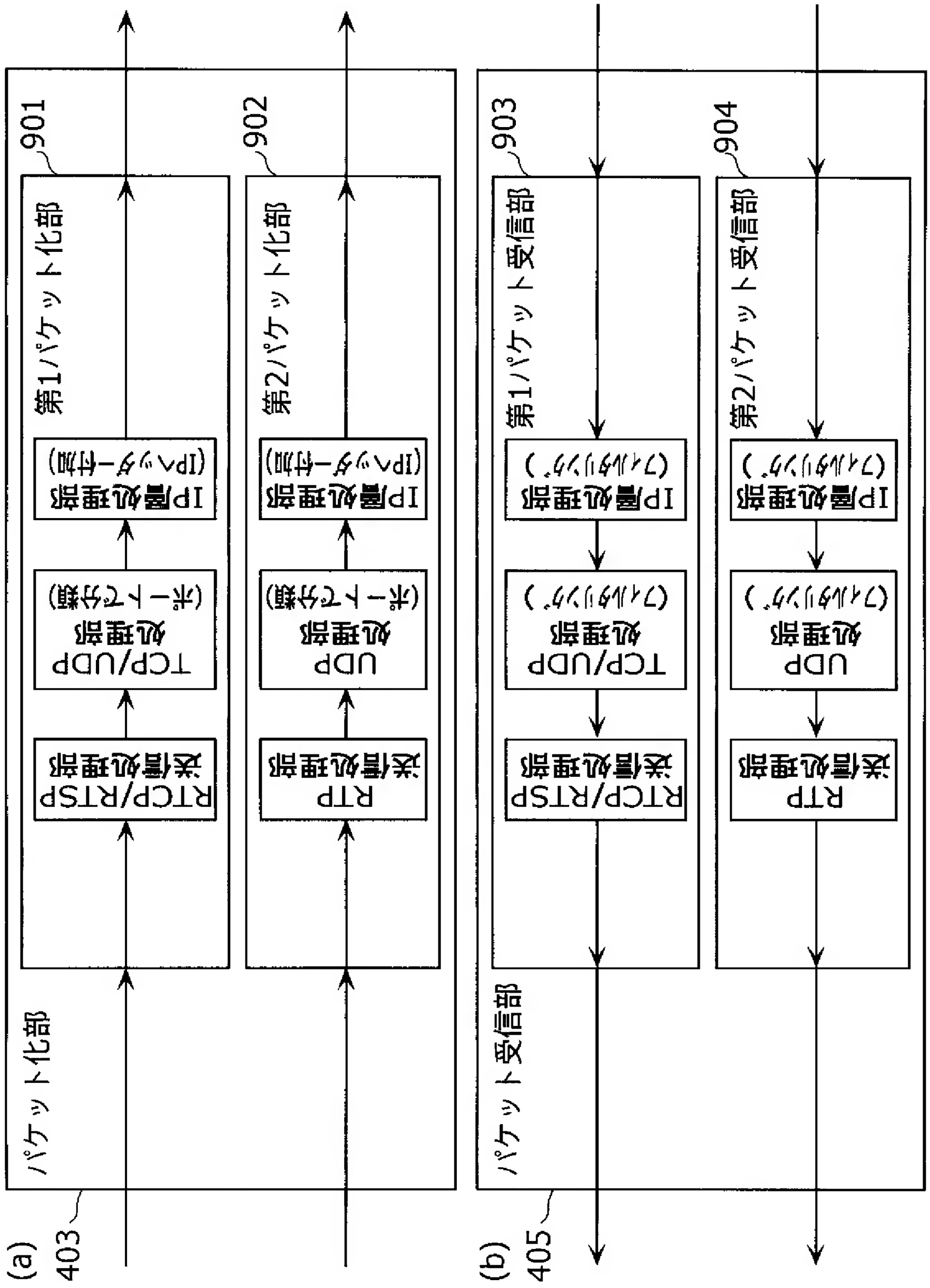
[図16]


6ビット 42ビット
BCID
Time-stamp
6バイト, 188バイト
TC
MPEG-TS
暗号化
暗号化されたTSデータ
暗号化情報ヘッダ
TCP/UDP ヘッダ
RTP ヘッダ
付加情報
暗号化されたTSデータ
10バイト
4ビット 64ビット 12ビット
EMI
シード情報
reserved
BCID: Base Clock ID
TC: Time-code
MPEG-TS: ISO/IEC 13818に準備
EMI: Encription Mode Indicator
O/E: Odd/Even
ただし、EMIおよびO/EはDTCPで規定されている。
DTCP:Digital Transmission Content Protection
DA: Destination Address
SA: Source Address
TPID: Tag Control ID
TCI: Tag Control Information
Priority: User Priority,使用法はISO/IEC 15802-3で規定
CFI: Canonical Format Indicator
VID: VLAN Identifier
イーサネットヘッダ
IPヘッダ
14バイト (802.1Q: 18バイト)
DA
SA
長さ/タイプ
6バイト 6バイト 2バイト
標準的なイーサネットヘッダ
802.1q拡張部
4バイト
TPID (新タイプ)
TCI (VLAN優先度)
2バイト 2バイト
(0x8100)
Priority
CFI
VID
3ビット 1ビット 12ビット
802.1qで拡張されたイーサネットヘッダ

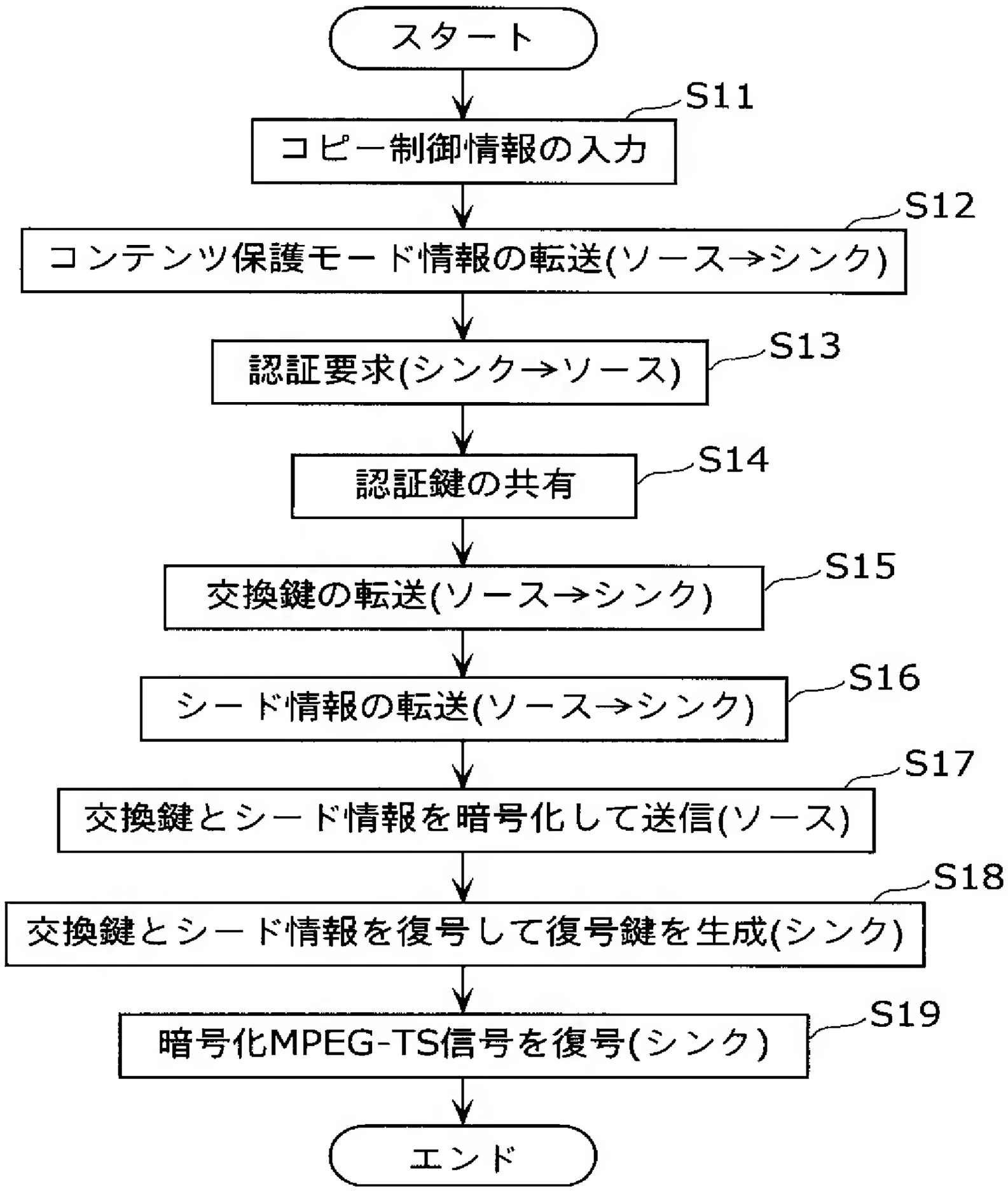
[図17]


401e
409
送信フレーム
410
受信フレーム
ソフトウェア化部
ソフトウェア受信部
602
603
601
403
403a
901
902
903
405a
904
405
第1キュー
第2キュー
送信キュー制御部
第1パケット化部
送信パケットに付加する情報の生成部
第2パケット化部
第1パケット受信部
受信パケットから付加情報を抽出する抽出部
第2パケット受信部
パケット送受信部
402
1201
1205
1206
407
DTCP情報生成部(EMI,シード情報)
O/E
暗号化鍵生成部
交換鍵生成部
鍵更新情報生成部
404
406
1204
暗号化データ生成部
復号鍵生成部
暗号化データ復号部
送信条件設定管理部
1203
1202
1207
408
AKEコマンド送信処理部
AKEコマンド受信処理部
受信条件設定管理部
送信条件の設定情報(送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル、リモート)
入力ストリーム(MPEG-TS)
EMI
DTCPパラメータ(設定情報)
出力ストリーム(MPEG-TS)
受信条件の設定情報(パラメータ、受信品質)

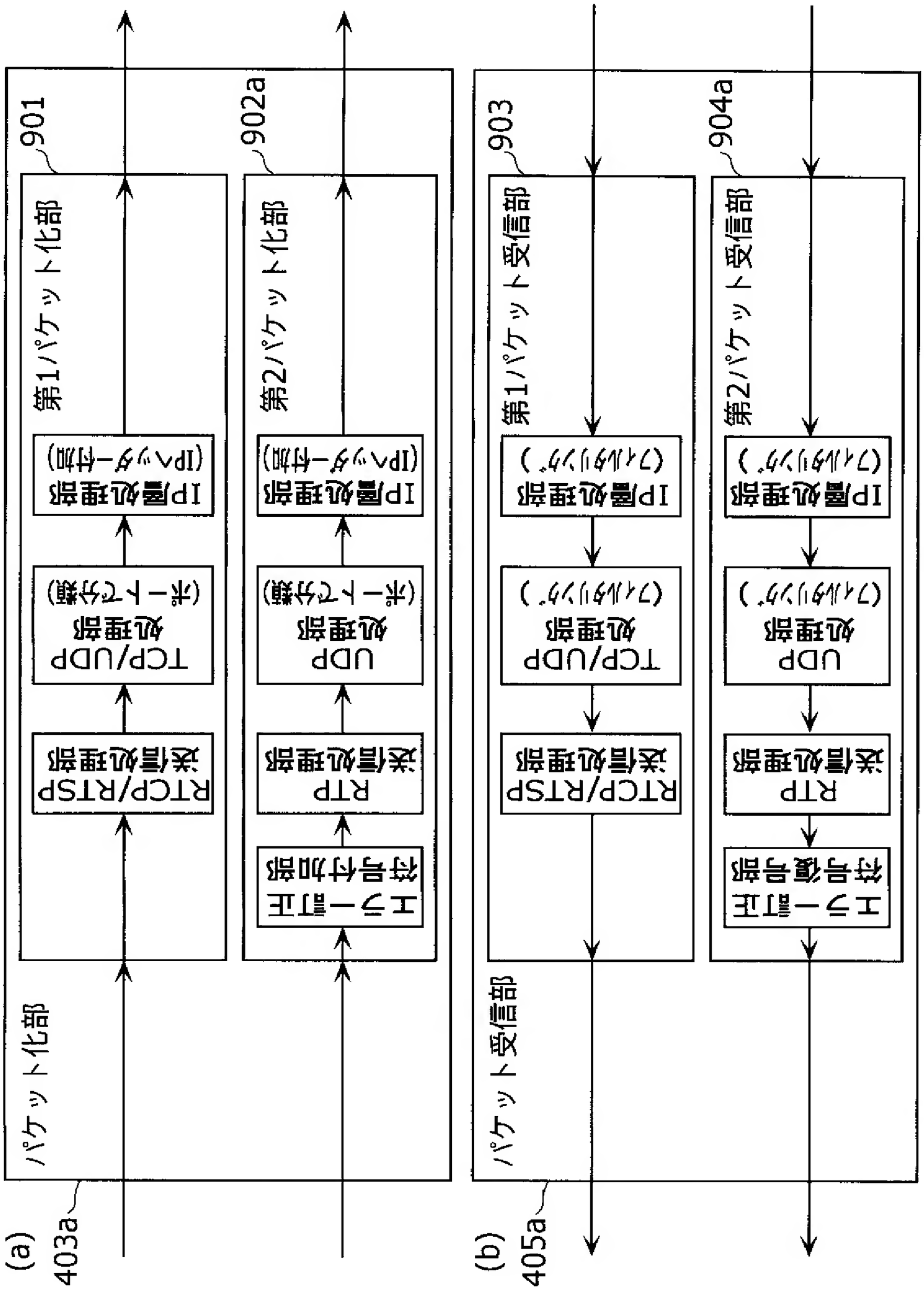
[図18]


(a)
403
パケット化部
901
902
第1パケット化部
第2パケット化部
RTCP/RTSP
送信処理部
TCP/UDP
処理部
(ポート下で分類)
IP層処理部
(IPヘッダ付加)
RTP
送信処理部
UDP
処理部
(ポート下で分類)
IP層処理部
(IPヘッダ付加)
(b)
405
パケット受信部
903
904
第1パケット受信部
第2パケット受信部
RTCP/RTSP
送信処理部
TCP/UDP
処理部
(フィルタリング)
IP層処理部
(フィルタリング)
RTP
送信処理部
UDP
処理部
(フィルタリング)
IP層処理部
(フィルタリング)

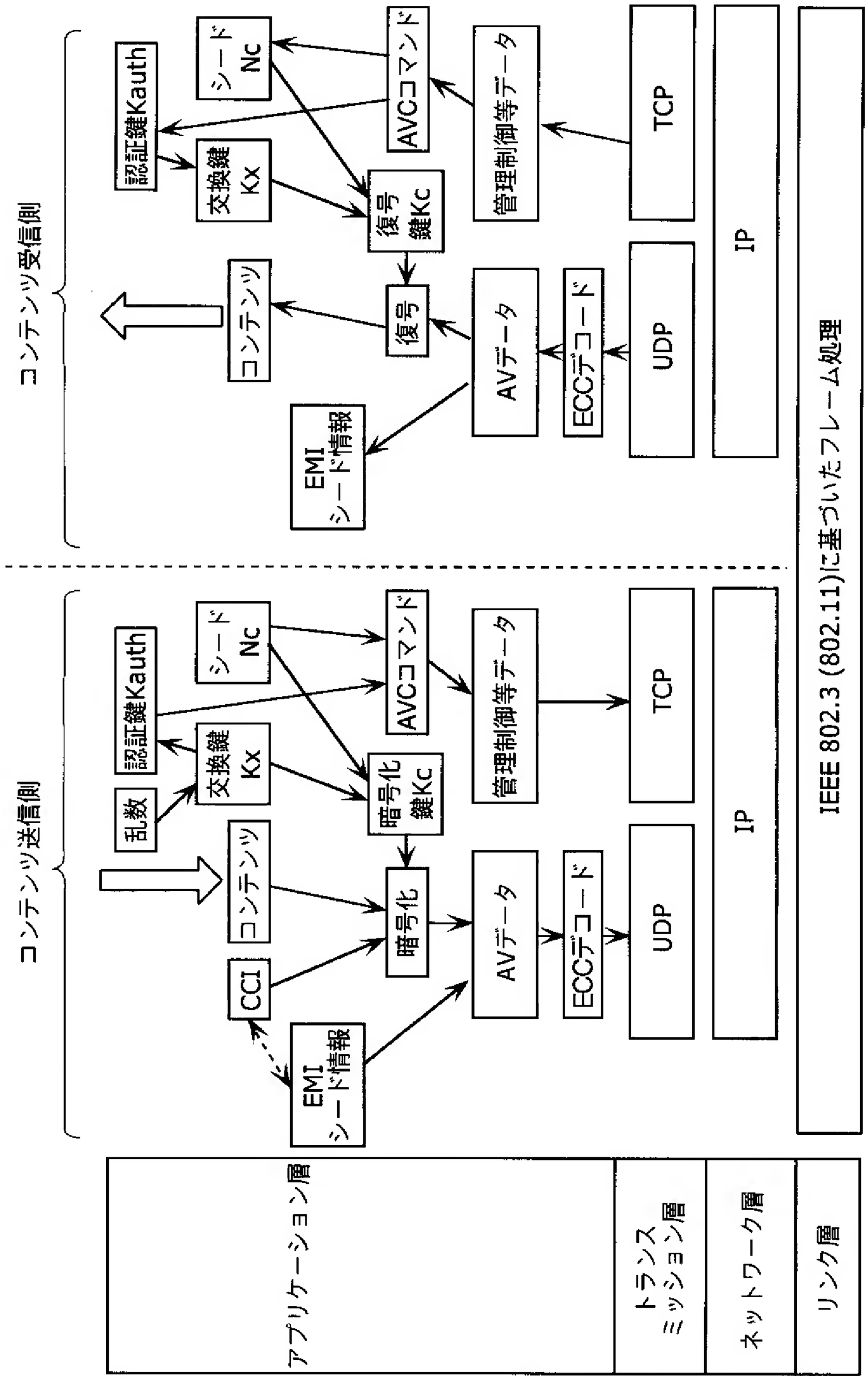
[図19]


スタート
S11
コピー制御情報の入力
S12
コンテンツ保護モード情報の転送(ソース→シンク)
S13
認証要求(シンク→ソース)
S14
認証鍵の共有
S15
交換鍵の転送(ソース→シンク)
S16
シード情報の転送(ソース→シンク)
S17
交換鍵とシード情報を暗号化して送信(ソース)
S18
交換鍵とシード情報を復号して復号鍵を生成(シンク)
S19
暗号化MPEG-TS信号を復号(シンク)
エンド

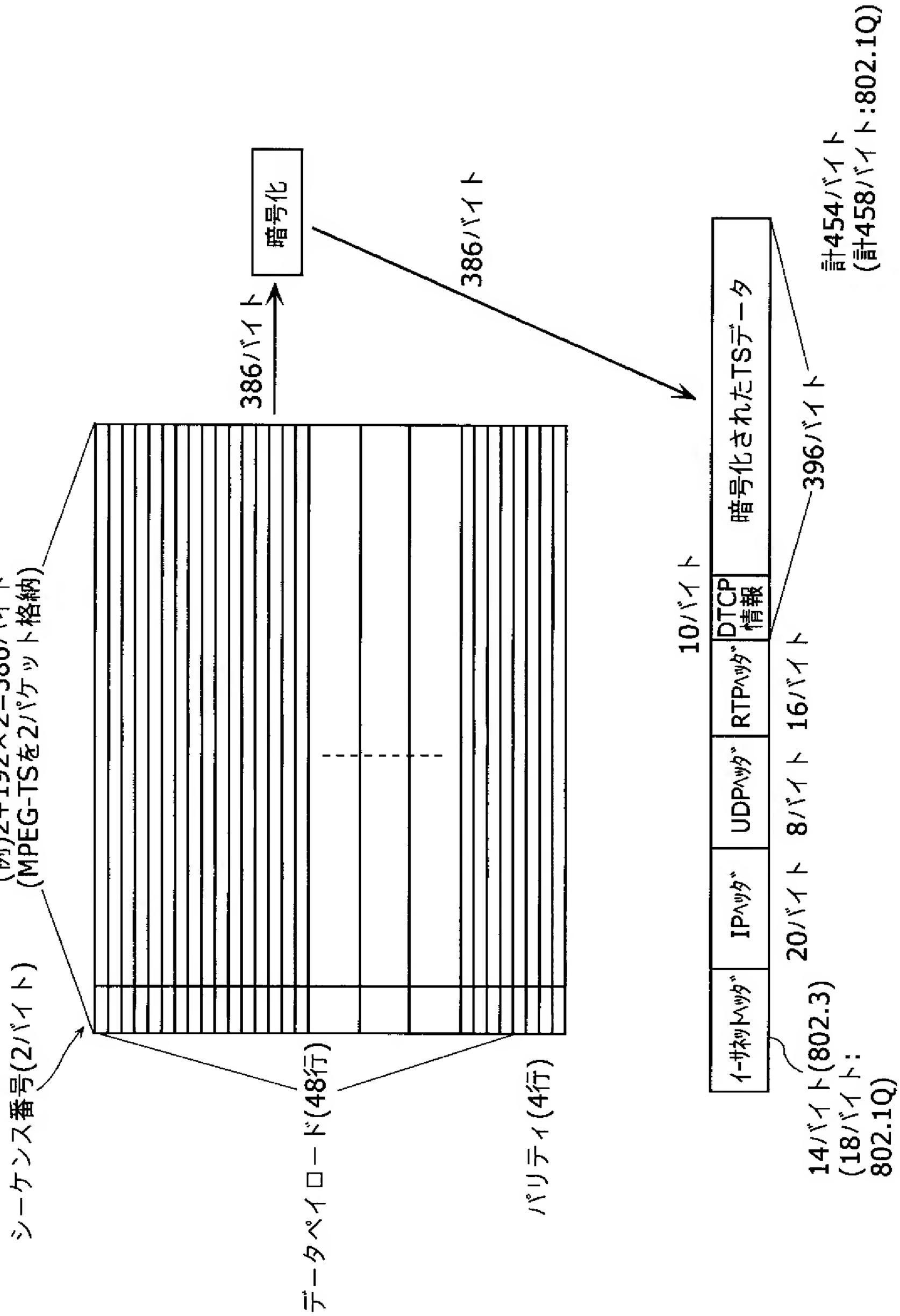
[図20]


(a)
403a
パケット化部
901
第1パケット化部
902a
第2パケット化部
TCP/UDP処理部(ポート番号分類)
RTCP/RTSP送信処理部
IP層処理部(IPヘッダ付加)
エラー訂正符号付加部
RTP送信処理部
UDP処理部(ポート番号分類)
IP層処理部(IPヘッダ付加)
(b)
405a
パケット受信部
903
第1パケット受信部
904a
第2パケット受信部
TCP/UDP処理部(フィルタリング)
RTCP/RTSP送信処理部
IP層処理部(フィルタリング)
エラー訂正符号復号部
RTP送信処理部
UDP処理部(フィルタリング)
IP層処理部(フィルタリング)

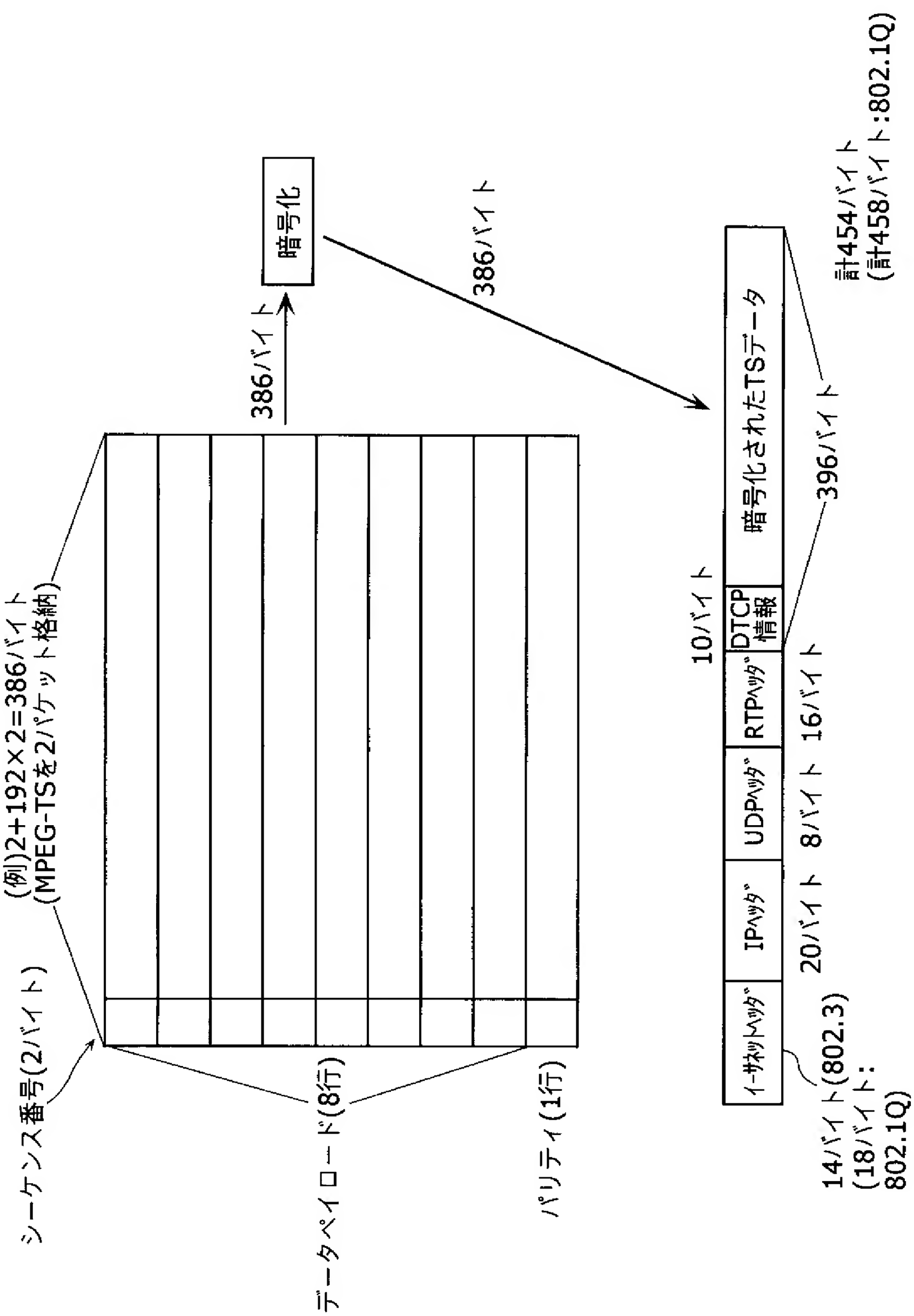
[図21]


コンテンツ受信側
認証鍵Kauth
シード Nc
交換鍵 Kx
AVCコマンド
管理制御等データ
TCP
IP
復号鍵Kc
コンテンツ
復号
AVデータ
ECCデコード
UDP
EMI シード情報
コンテンツ送信側
乱数
暗号化鍵Kc
暗号化
CCI
アプリケーション層
トランスミッション層
ネットワーク層
リンク層
IEEE 802.3 (802.11)に基づいたフレーム処理

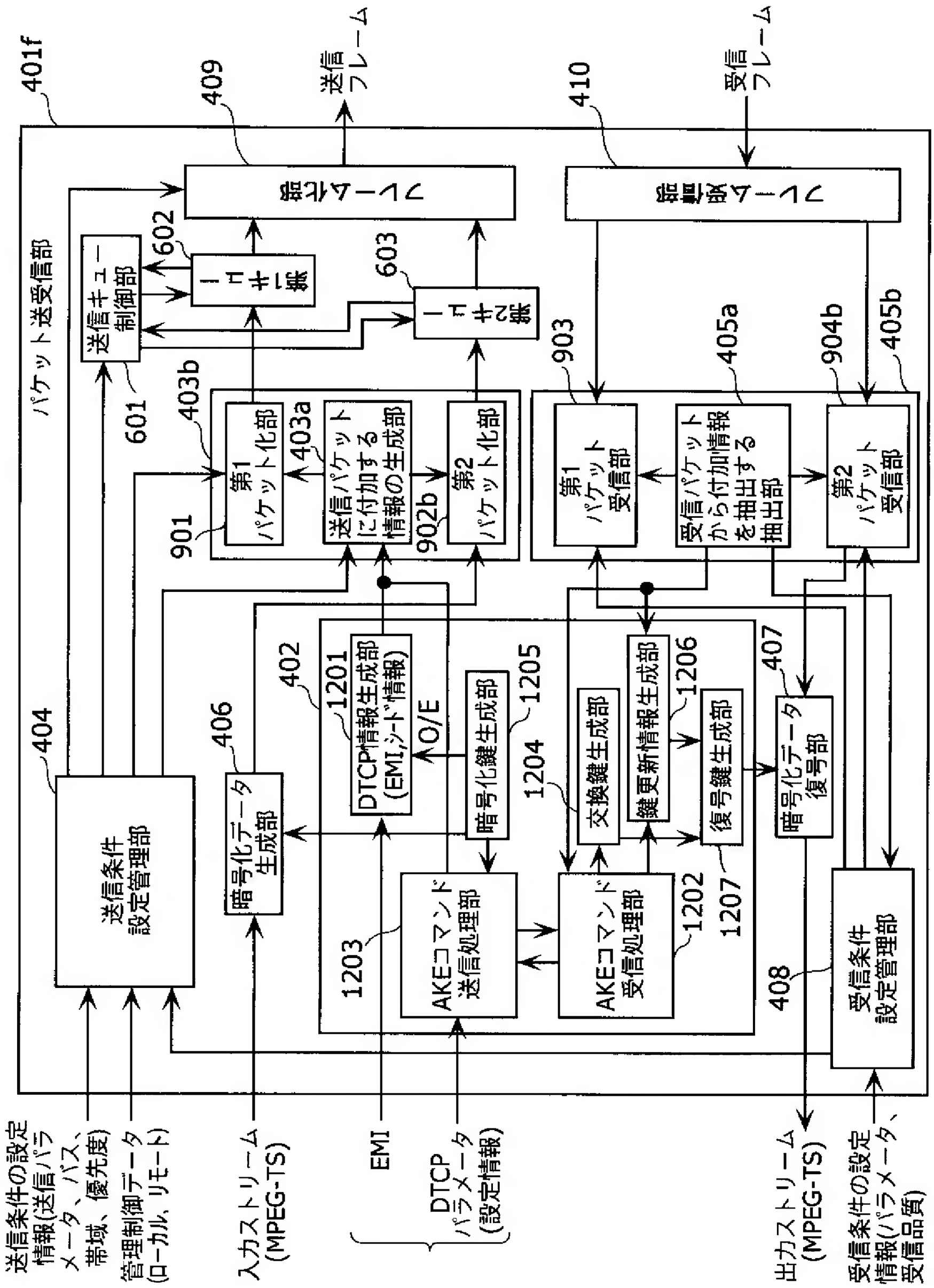
[図22]


暗号化
386バイト
386バイト
(例)2+192×2=386バイト
(MPEG-TSを2パケット格納)
シーケンス番号(2バイト)
データペイロード(48行)
パリティ(4行)
計454バイト
(計458バイト:802.1Q)
暗号化されたTSデータ
DTCP情報
396バイト
10バイト
RTPﾍｯﾀﾞ
UDPﾍｯﾀﾞ
IPﾍｯﾀﾞ
ｲｰｻﾈｯﾄﾍｯﾀﾞ
20バイト 8バイト 16バイト
14バイト(802.3)
(18バイト:
802.1Q)

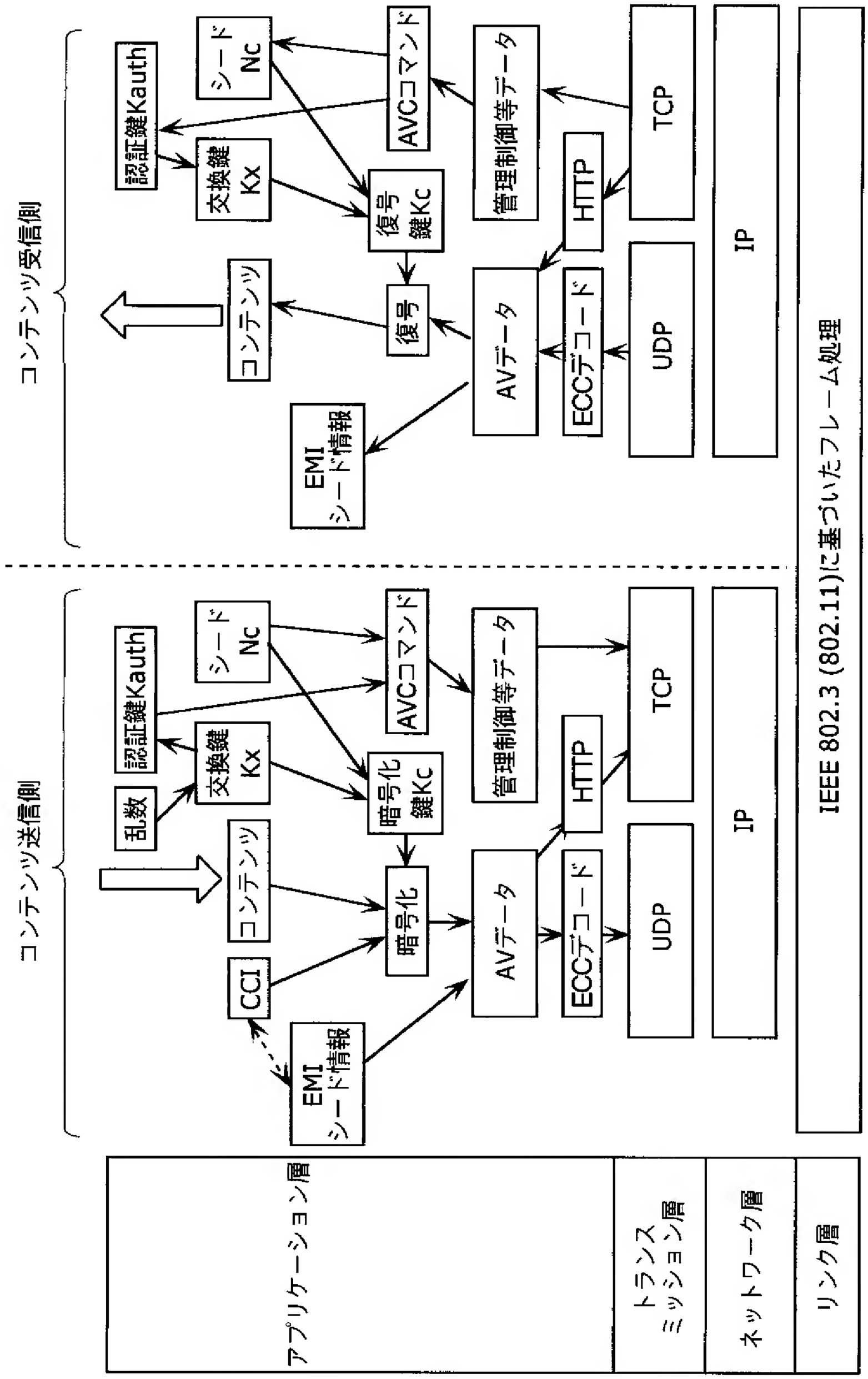
[図23]


暗号化
386バイト
386バイト
(例)2+192×2=386バイト
(MPEG-TSを2パケット格納)
シーケンス番号(2バイト)
データペイロード(8行)
パリティ(1行)
計454バイト
(計458バイト:802.1Q)
暗号化されたTSデータ
DTCP情報
RTPﾍｯﾀﾞ
UDPﾍｯﾀﾞ
IPﾍｯﾀﾞ
ｲｰｻﾈｯﾄﾍｯﾀﾞ
10バイト
20バイト
8バイト
16バイト
396バイト
14バイト(802.3)
(18バイト:
802.1Q)

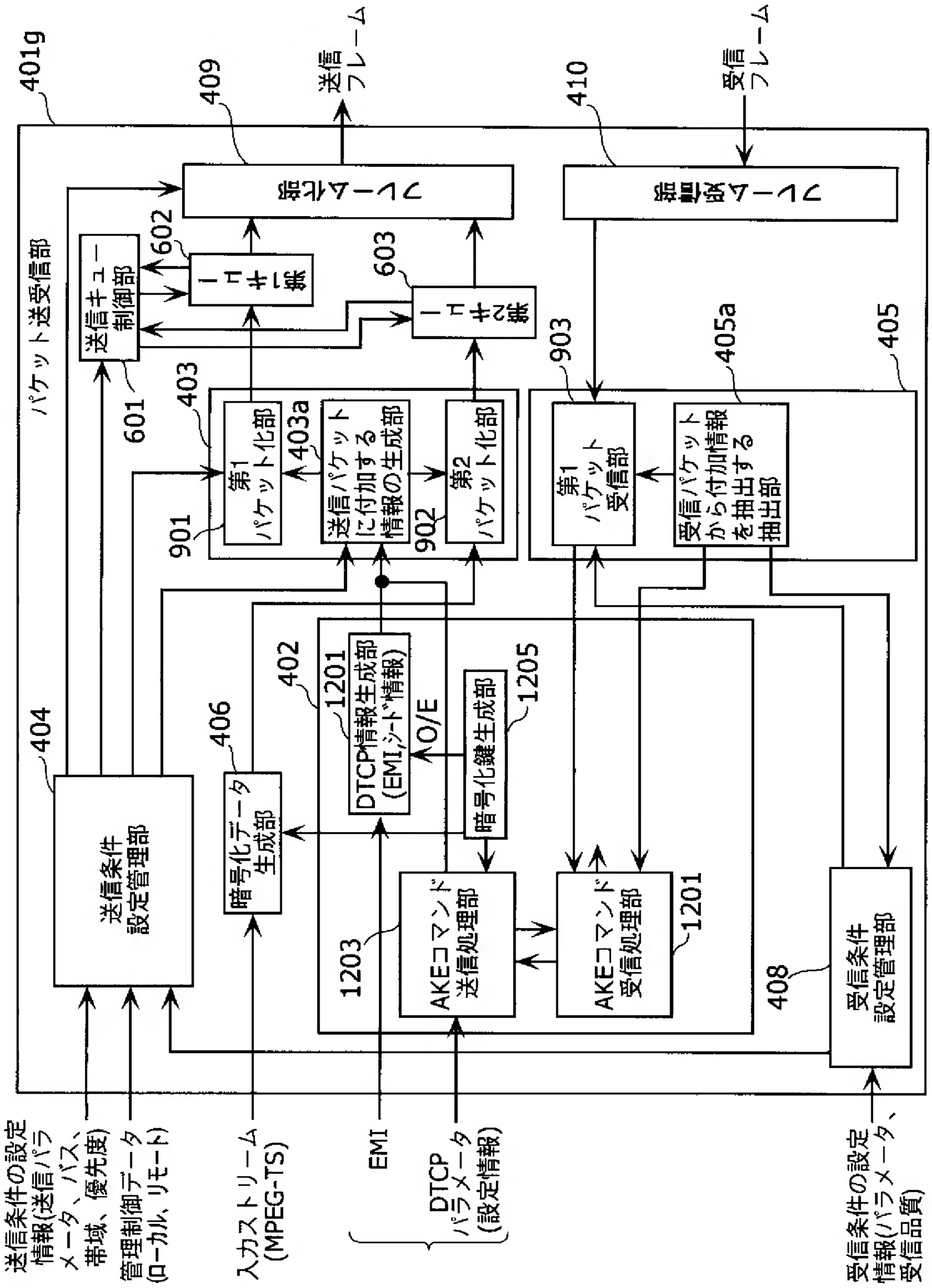
[図24]


401f
409
送信フレーム
410
受信フレーム
フレーム化部
フレーム受信部
パケット送受信部
送信キュー制御部
602
第1キュー
603
第2キュー
601
403b
第1パケット化部
403a
送信パケットに付加する情報の生成部
902b
第2パケット化部
901
第1パケット受信部
受信パケットから付加情報を抽出する抽出部
903
405a
904b
405b
第2パケット受信部
404
送信条件設定管理部
406
暗号化データ生成部
402
1201
DTCP情報生成部(EMI,シード情報)
O/E
暗号化鍵生成部
1205
1204
交換鍵生成部
鍵更新情報生成部
1206
復号鍵生成部
407
暗号化データ復号部
1203
AKEコマンド送信処理部
AKEコマンド受信処理部
1202
1207
408
受信条件設定管理部
送信条件の設定情報(送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル、リモート)
入力ストリーム(MPEG-TS)
EMI
DTCPパラメータ(設定情報)
出力ストリーム(MPEG-TS)
受信条件の設定情報(パラメータ、受信品質)

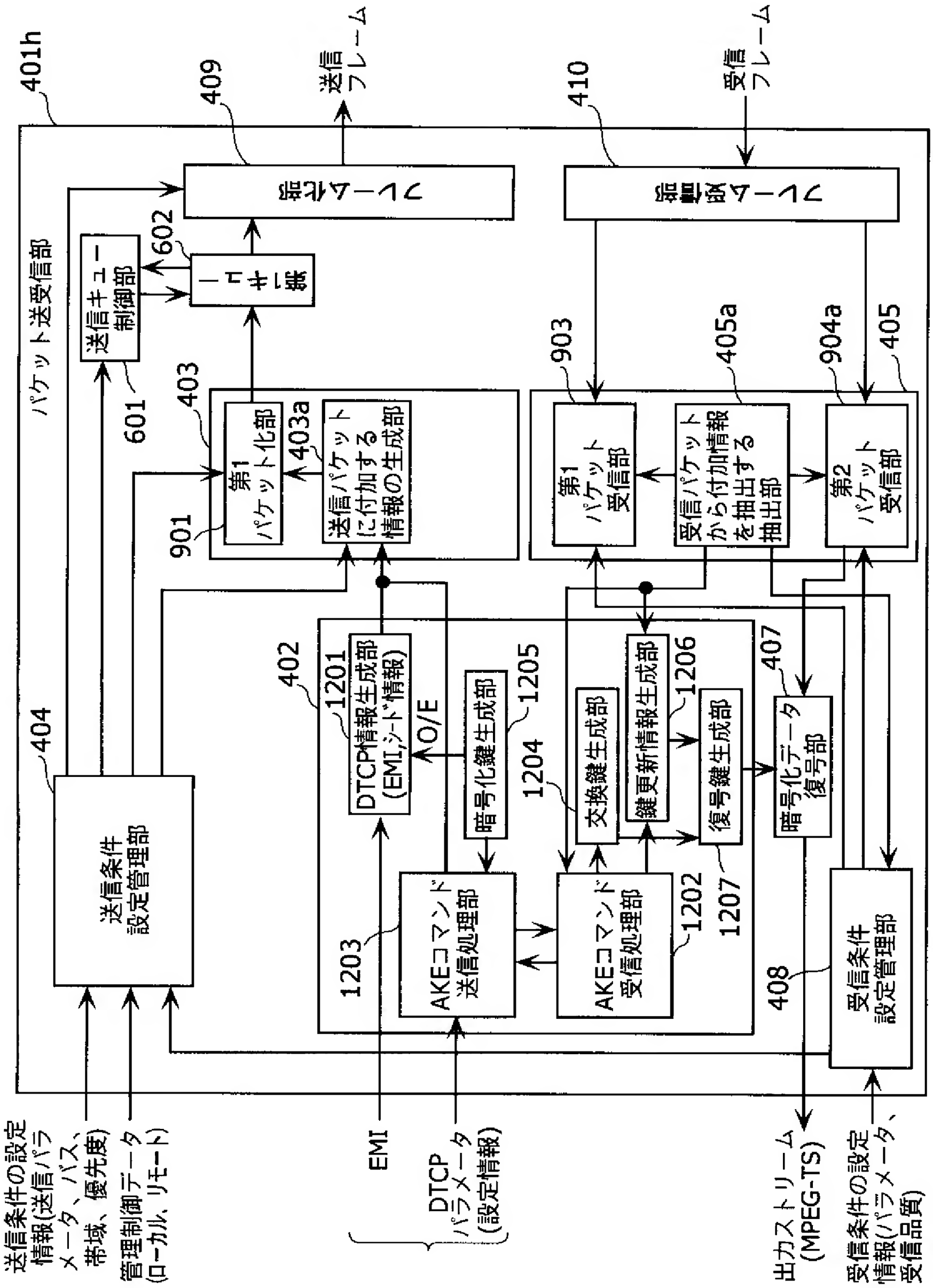
[図25]


コンテンツ受信側
認証鍵Kauth
シード Nc
交換鍵 Kx
復号 鍵Kc
AVCコマンド
管理制御等データ
TCP
HTTP
IP
コンテンツ
復号
AVデータ
ECCデコード
UDP
EMI シード情報
IEEE 802.3 (802.11)に基づいたフレーム処理
コンテンツ送信側
乱数
認証鍵Kauth
シード Nc
交換鍵 Kx
暗号化 鍵Kc
AVCコマンド
管理制御等データ
TCP
HTTP
IP
コンテンツ
CCI
暗号化
AVデータ
ECCデコード
UDP
EMI シード情報
アプリケーション層
トランスミッション層
ネットワーク層
リンク層

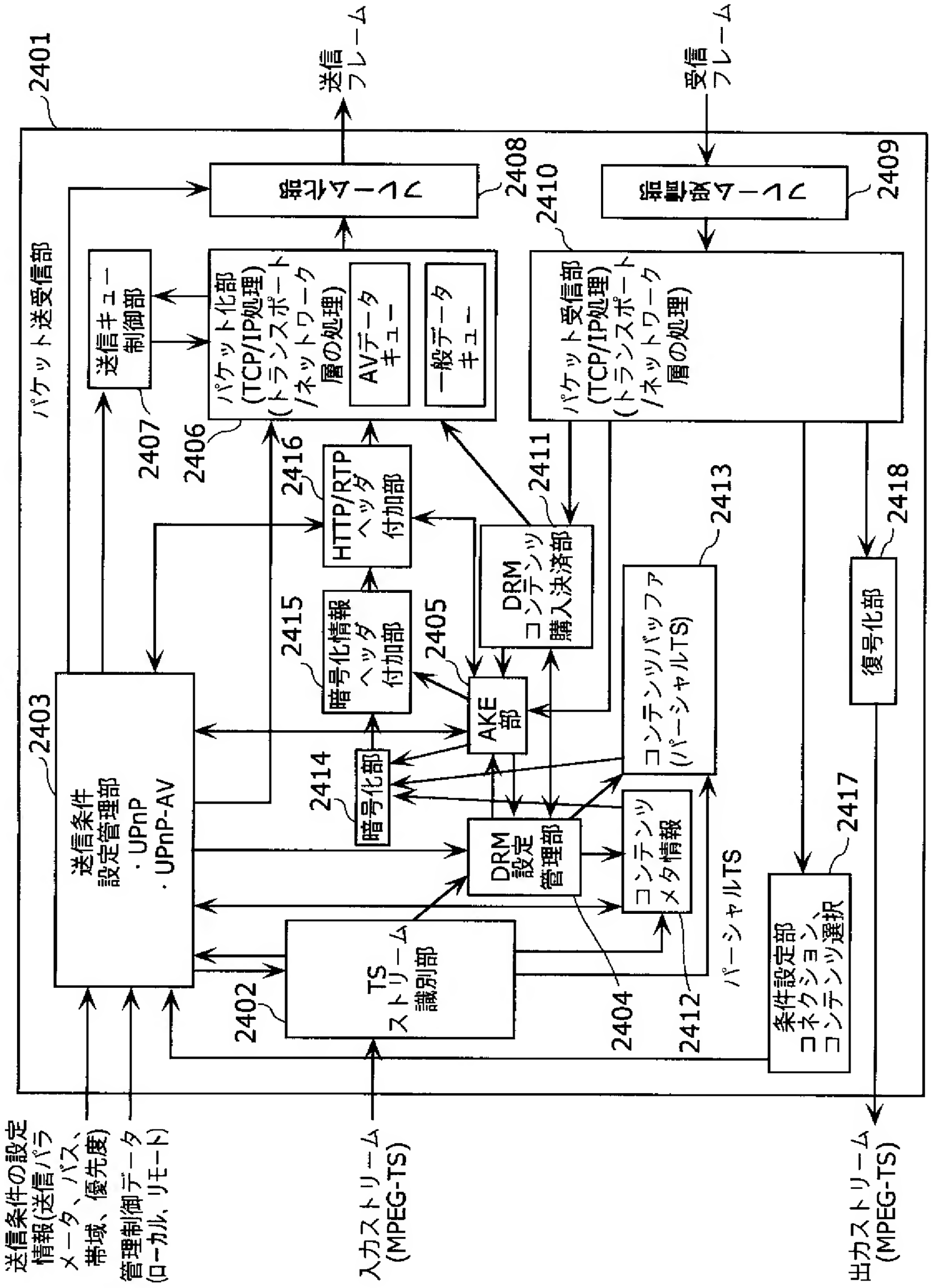
[図26]


401g
409
送信フレーム
410
受信フレーム
ストリーム化部
ストリーム受信部
602
603
送信キュー制御部
第1キュー
第2キュー
601
903
405a
405
403
403a
901
902
第1パケット化部
送信パケットに付加する情報の生成部
第2パケット化部
第1パケット受信部
受信パケットから付加情報を抽出する抽出部
402
1201
DTCP情報生成部(EMI,シード情報)
O/E
1205
暗号化鍵生成部
404
406
送信条件設定管理部
暗号化データ生成部
1203
AKEコマンド送信処理部
AKEコマンド受信処理部
1201
408
受信条件設定管理部
送信条件の設定情報(送信パラメータ、バス、帯域、優先度)
管理制御データ(ローカル、リモート)
入力ストリーム(MPEG-TS)
EMI
DTCPパラメータ(設定情報)
受信条件の設定情報(パラメータ、受信品質)

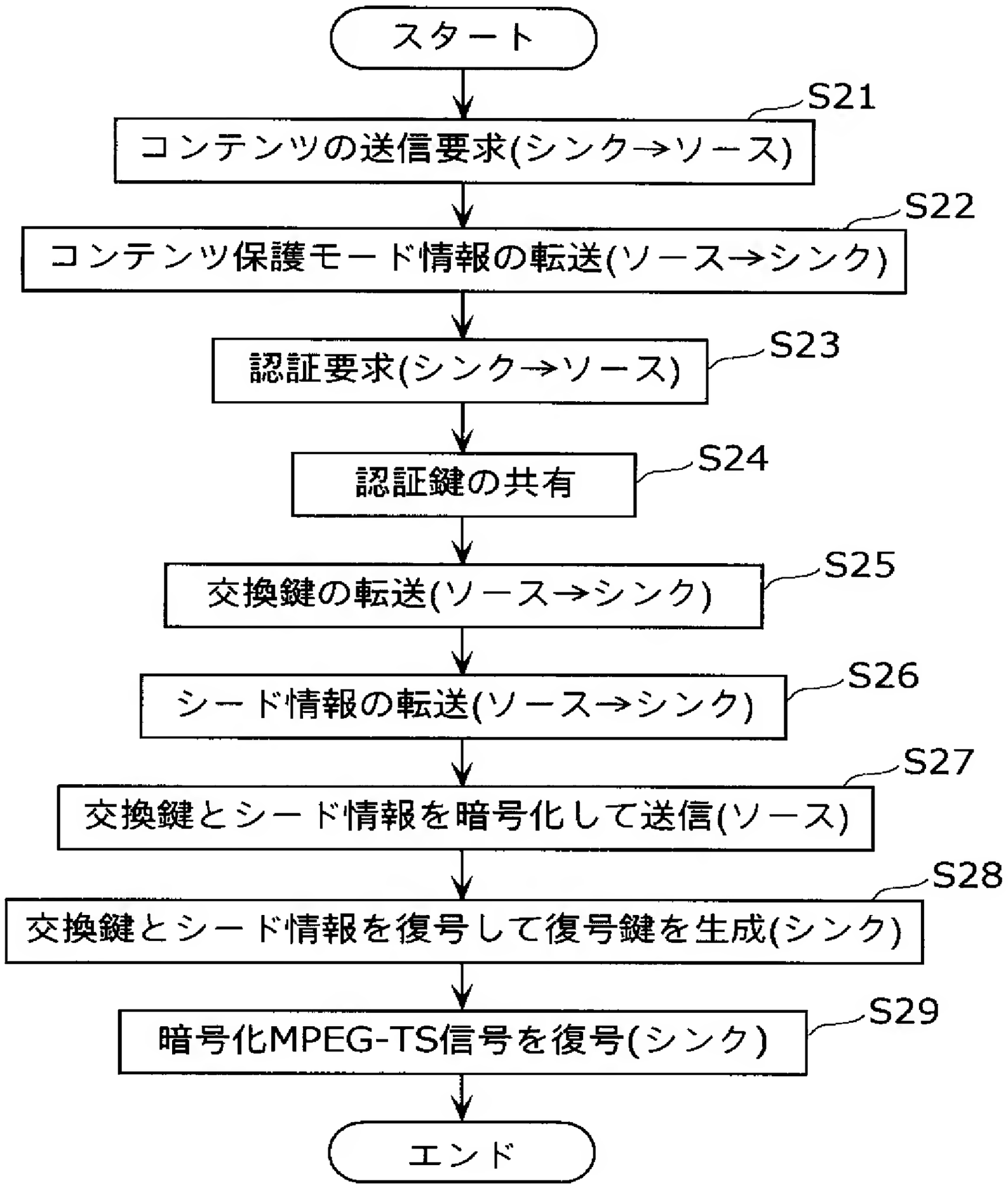
[図27]


401h
409
送信フレーム
410
受信フレーム
パケット送受信部
送信条件設定管理部
送信キュー制御部
602
第1キュー
601
403
第1パケット化部
403a
送信パケットに付加する情報の生成部
901
フレーム化部
フレーム受信部
903
第1パケット受信部
405a
受信パケットから付加情報を抽出する抽出部
904a
第2パケット受信部
405
404
402
1201
DTCP情報生成部(EMI,シード情報)
O/E
暗号化鍵生成部
1205
1204
交換鍵生成部
鍵更新情報生成部
1206
復号鍵生成部
407
暗号化データ復号部
1203
AKEコマンド送信処理部
AKEコマンド受信処理部
1202
1207
408
受信条件設定管理部
送信条件の設定情報(送信パラメータ、バス、帯域、優先度)
管理制御データ(ローカル、リモート)
EMI
DTCPパラメータ(設定情報)
出力ストリーム(MPEG-TS)
受信条件の設定情報(パラメータ、受信品質)

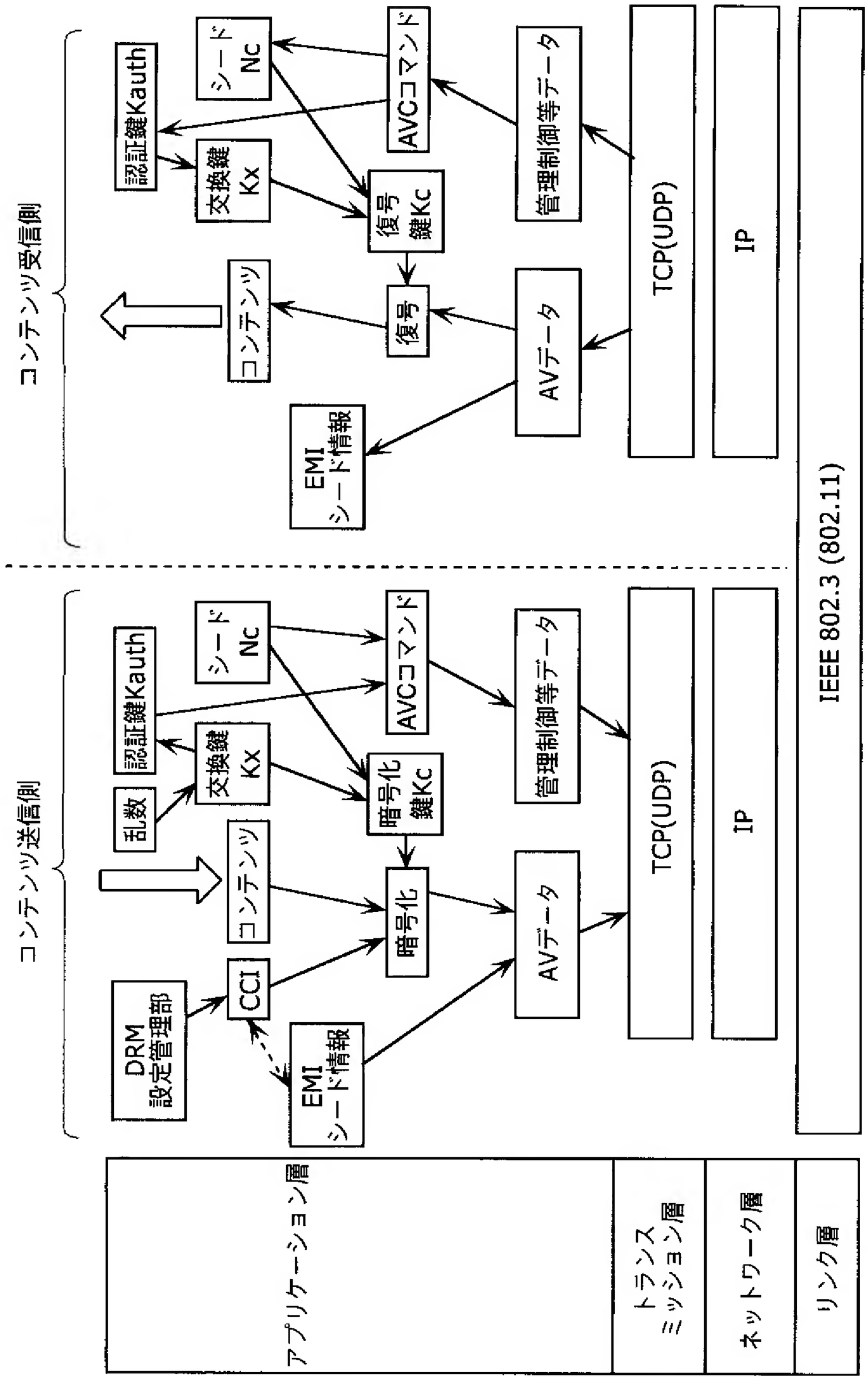
[図28]


2401
送信フレーム
受信フレーム
2408
2410
2409
パケット送受信部
送信キュー制御部
パケット化部(TCP/IP処理)(トランスポート/ネットワーク層の処理)
AVデータキュー
一般データキュー
パケット受信部(TCP/IP処理)(トランスポート/ネットワーク層の処理)
2407
2406
2416
HTTP/RTPヘッダ付加部
2411
2413
2418
2415
暗号化情報ヘッダ付加部
2405
DRMコンテンツ購入決済部
コンテンツバッファ(パーシャルTS)
復号化部
2403
送信条件設定管理部
・UPnP
・UPnP-AV
AKE部
2414
暗号化部
DRM設定管理部
コンテンツメタ情報
2417
条件設定部
コネクション、
コンテンツ選択
2402
TSストリーム識別部
2404
2412
パーシャルTS
送信条件の設定情報(送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル、リモート)
入力ストリーム(MPEG-TS)
出力ストリーム(MPEG-TS)

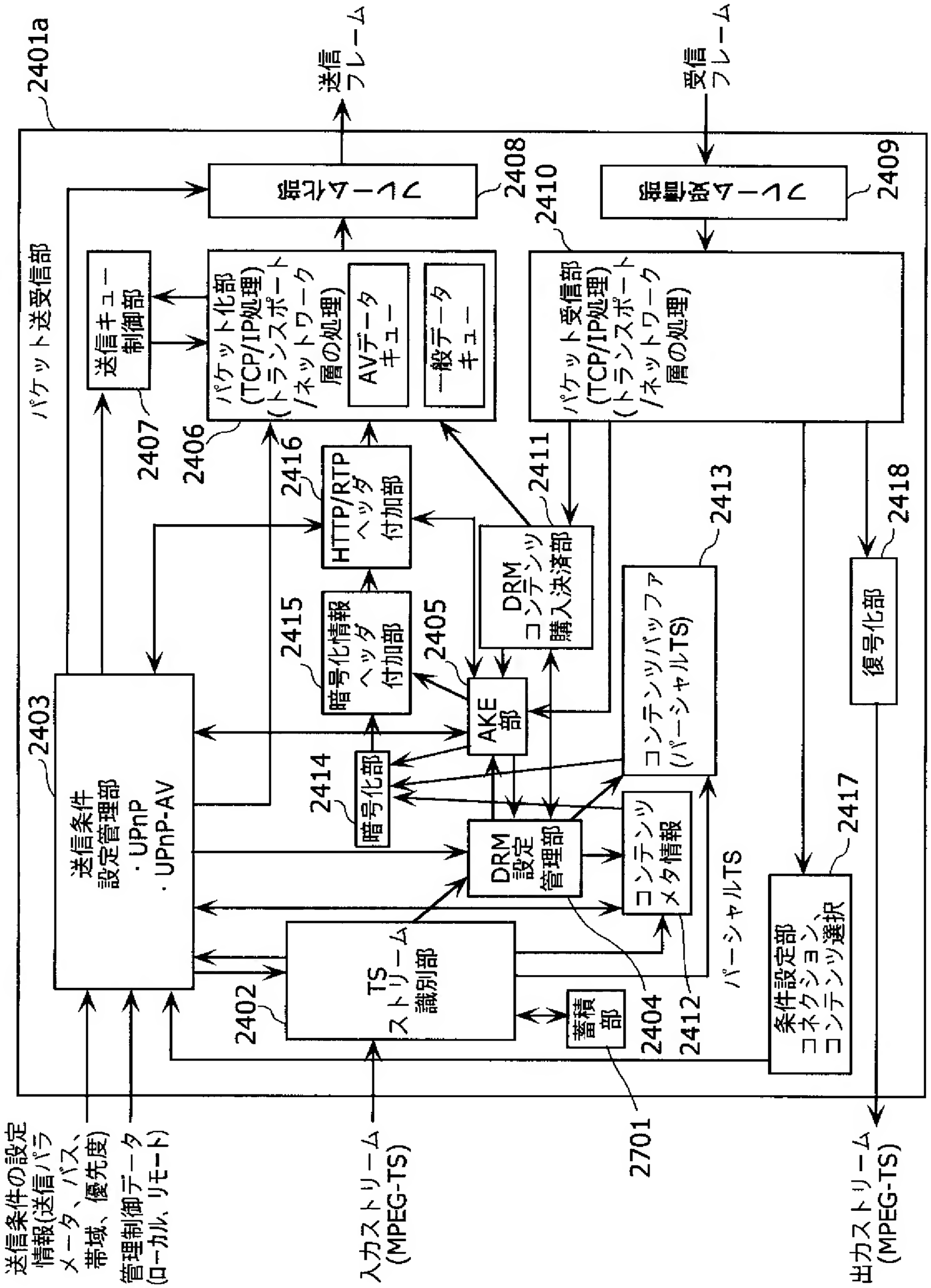
[図29]


スタート
S21
コンテンツの送信要求(シンク→ソース)
S22
コンテンツ保護モード情報の転送(ソース→シンク)
S23
認証要求(シンク→ソース)
S24
認証鍵の共有
S25
交換鍵の転送(ソース→シンク)
S26
シード情報の転送(ソース→シンク)
S27
交換鍵とシード情報を暗号化して送信(ソース)
S28
交換鍵とシード情報を復号して復号鍵を生成(シンク)
S29
暗号化MPEG-TS信号を復号(シンク)
エンド

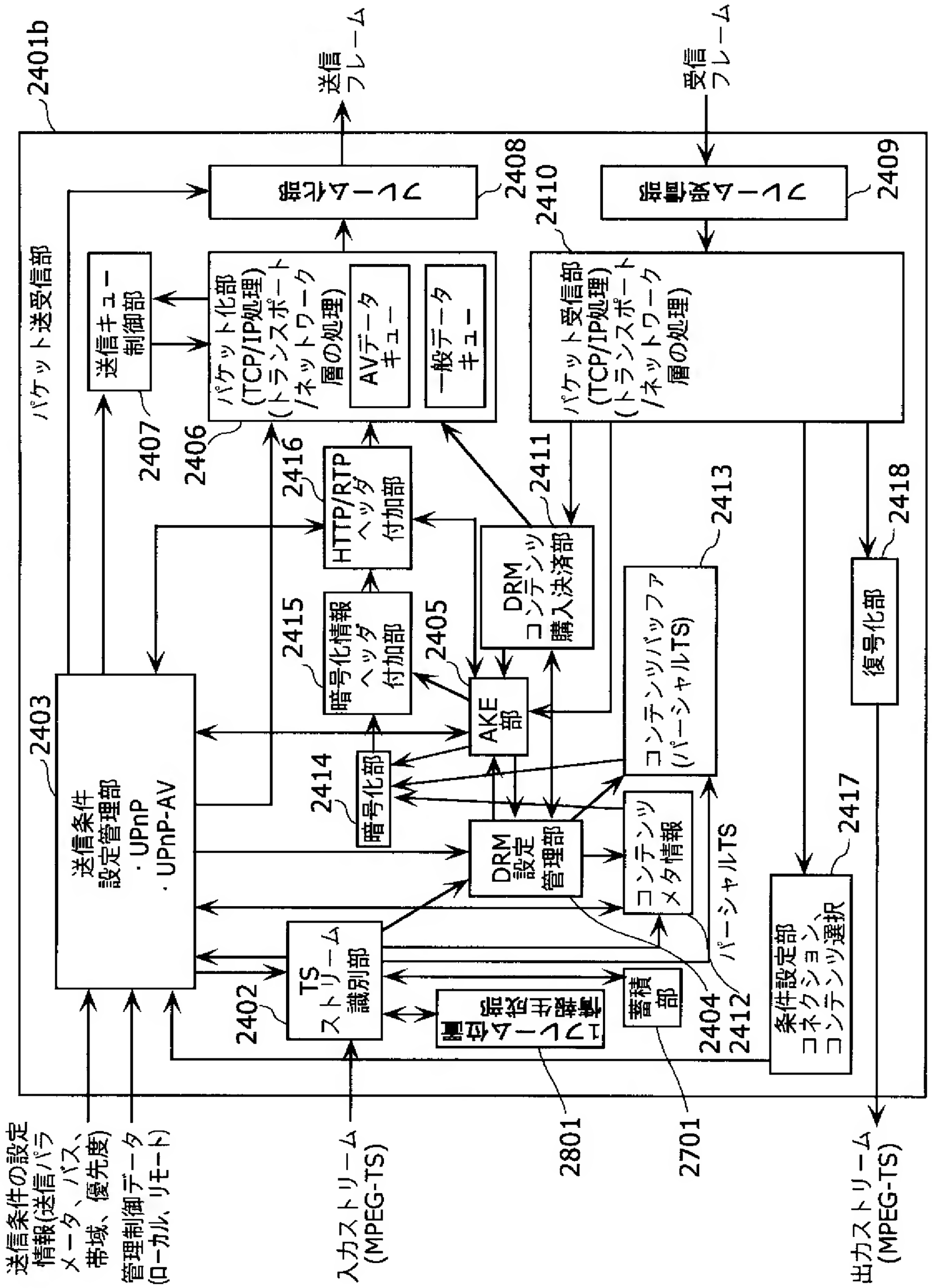
[図30]


コンテンツ受信側
認証鍵Kauth
シード Nc
交換鍵 Kx
AVCコマンド
復号 鍵Kc
管理制御等データ
TCP(UDP)
IP
コンテンツ
復号
AVデータ
EMI シード情報
コンテンツ送信側
乱数
暗号化 鍵Kc
暗号化
DRM 設定管理部
CCI
アプリケーション層
トランス ミッション層
ネットワーク層
リンク層
IEEE 802.3 (802.11)

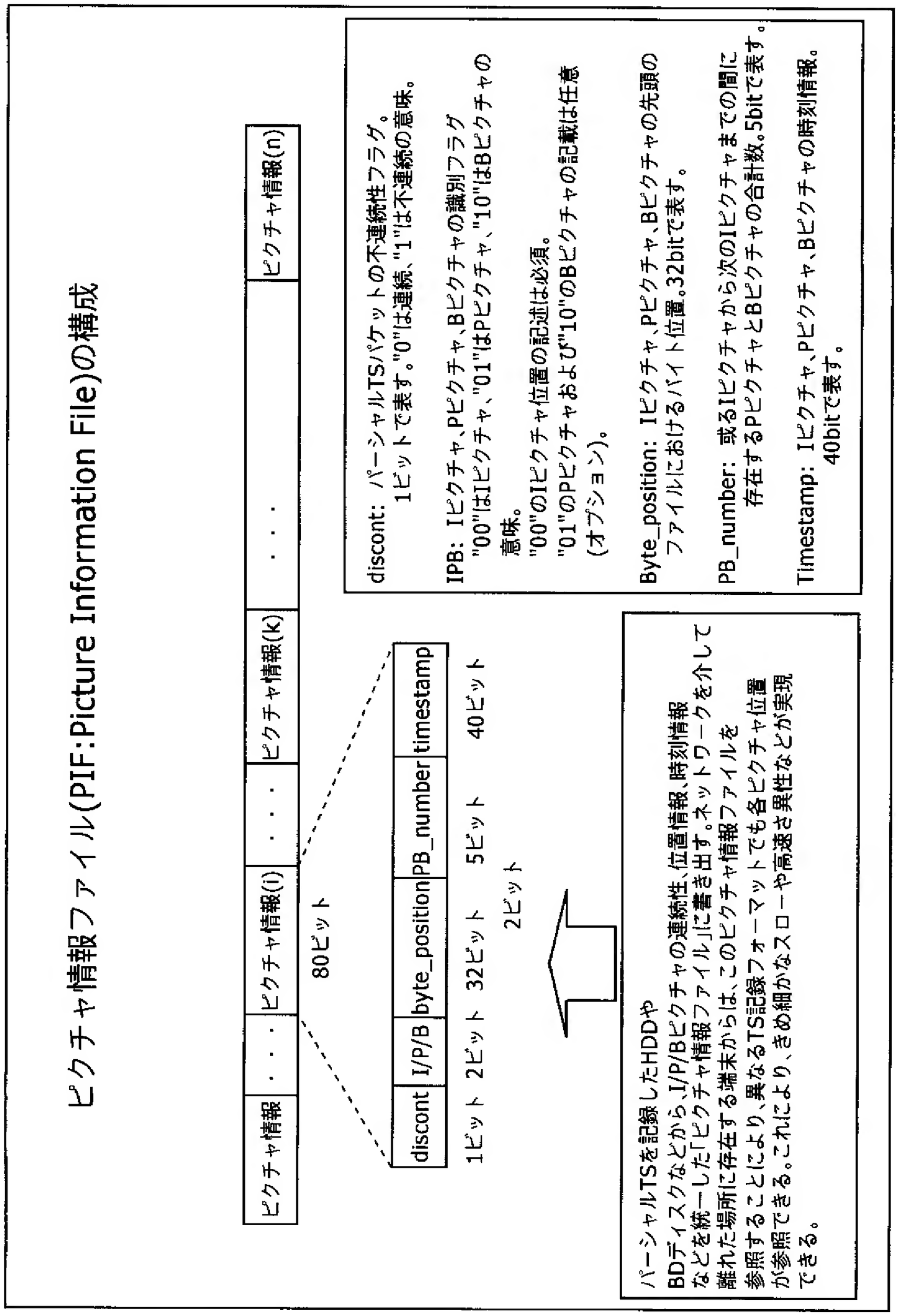
[図31]


2401a
送信フレーム
受信フレーム
パケット送受信部
2408
2409
2410
送信キュー制御部
パケット化部(TCP/IP処理)(トランスポート/ネットワーク層の処理)
AVデータキュー
一般データキュー
パケット受信部(TCP/IP処理)(トランスポート/ネットワーク層の処理)
2407
2406
2416
HTTP/RTP ヘッダ付加部
2411
2413
2418
2415
暗号化情報ヘッダ付加部
2405
DRM コンテンツ購入決済部
コンテンツバッファ(パーシャルTS)
復号化部
2403
送信条件設定管理部 ・UPnP ・UPnP-AV
AKE部
2414
暗号化部
DRM設定管理部
コンテンツメタ情報
2417
パーシャルTS
条件設定部 コネクション、コンテンツ選択
2402
TSストリーム識別部
蓄積部
2404
2412
2701
送信条件の設定情報(送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル、リモート)
入力ストリーム(MPEG-TS)
出力ストリーム(MPEG-TS)

[図32]


2401b
送信フレーム
受信フレーム
パケット送受信部
2408
2409
2410
送信キュー制御部
パケット化部(TCP/IP処理)(トランスポート/ネットワーク層の処理)
AVデータキュー
一般データキュー
パケット受信部(TCP/IP処理)(トランスポート/ネットワーク層の処理)
2407
2406
2416
HTTP/RTPヘッダ付加部
2411
2413
2418
2415
暗号化情報ヘッダ付加部
2405
DRMコンテンツ購入決済部
コンテンツバッファ(パーシャルTS)
復号化部
2403
送信条件設定管理部
・UPnP
・UPnP-AV
AKE部
2414
暗号化部
DRM設定管理部
コンテンツメタ情報
パーシャルTS
2417
2402
TSストリーム識別部
トレーサビリティ情報生成部
蓄積部
2404
2412
条件設定部
コネクション、
コンテンツ選択
送信条件の設定情報(送信パラメータ、パス、帯域、優先度)
管理制御データ(ローカル、リモート)
入力ストリーム(MPEG-TS)
2801
2701
出力ストリーム(MPEG-TS)

[図33]


ピクチャ情報ファイル(PIF:Picture Information File)の構成
ピクチャ情報(n)
ピクチャ情報(k)
ピクチャ情報(i)
discont: パーシャルTS/パケットの不連続性フラグ。
1ビットで表す。"0"は連続、"1"は不連続の意味。
IPB: IピクチャPピクチャ、Bピクチャの識別フラグ
"00"はIピクチャ、"01"はPピクチャ、"10"はBピクチャの意味。
"00"のIピクチャ位置の記述は必須。
"01"のPピクチャおよび"10"のBピクチャの記載は任意
(オプション)。
Byte_position: Iピクチャ、Pピクチャ、Bピクチャの先頭のファイルにおけるバイト位置。32bitで表す。
PB_number: 或るIピクチャから次のIピクチャまでの間に存在するPピクチャとBピクチャの合計数。5bitで表す。
Timestamp: Iピクチャ、Pピクチャ、Bピクチャの時刻情報。40bitで表す。
ピクチャ情報
80ビット
discont
I/P/B
byte_position
PB_number
timestamp
1ビット 2ビット 32ビット 5ビット 40ビット
2ビット
パーシャルTSを記録したHDDやBDディスクなどから、I/P/Bピクチャの連続性、位置情報、時刻情報などを統一した「ピクチャ情報ファイル」に書き出す。ネットワークを介して離れた場所に存在する端末からは、このピクチャ情報ファイルを参照することにより、異なるTS記録フォーマットでも各ピクチャ位置が参照できる。これにより、ネットワークやスローや高速さ異性などが実現できる。

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/018491

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/56

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/56

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho(Y1,Y2) 1922-1996 Toroku Jitsuyo Shinan Koho(U) 1994-2005
Kokai Jitsuyo Shinan Koho(U) 1971-2005 Jitsuyo Shinan Toroku Koho(Y2) 1996-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-285283 A (Toshiba Corp.), 12 October, 2001 (12.10.01), Abstract; Claims; Par. No. [0011] (Family: none)	1-41
Y	JP 11-341040 A (Toshiba Corp.), 10 December, 1999 (10.12.99), Abstract; Claims & JP 3571912 B2	1-41
Y	JP 2001-127785 A (Toshiba Corp.), 11 May, 2001 (11.05.01), Abstract; Claims; Par. No. [0137] (Family: none)	1-41

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 March, 2005 (08.03.05)	29 March, 2005 (29.03.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/018491

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 4-223787 A (GTE Laboratories Inc.), 13 August, 1992 (13.08.92), Abstract & US 5046090 A	1-41

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１８４９１

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ　１２／５６

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ　１２／５６

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報（Ｙ１，Ｙ２）	１９２２－１９９６年
日本国公開実用新案公報（U）	１９７１－２００５年
日本国登録実用新案公報（U）	１９９４－２００５年
日本国実用新案登録公報（Ｙ２）	１９９６－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　２００１－２８５２８３　Ａ（株式会社東芝），２００１．１０．１２，要約、特許請求の範囲、段落１１（ファミリなし）	１－４１
Ｙ	ＪＰ　１１－３４１０４０　Ａ（株式会社東芝），１９９９．１２．１０，要約、特許請求の範囲 & ＪＰ　３５７１９１２　Ｂ２	１－４１
Ｙ	ＪＰ　２００１－１２７７８５　Ａ（株式会社東芝），２００１．０５．１１，要約、特許請求の範囲、段落１３７	１－４１

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　０８．０３．２００５	国際調査報告の発送日　29.3.2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｘ　４２４０ 小林紀和 電話番号　０３－３５８１－１１０１　内線　３５５６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
	（ファミリなし）	
Ｙ	ＪＰ　４－２２３７８７　Ａ（ジー・テイー・イー・ラボラトリーズ・インコーポレイテツド），１９９２．０８．１３，要約 ＆　ＵＳ　５０４６０９０　Ａ	１－４１